U.S. NAVAL ACADEMY
COMPUTER SCIENCE DEPARTMENT
TECHNICAL REPORT

Initial Report of the Dean's Cyber Warfare Ad Hoc Committee

Needham, Donald M Vincent, Patrick J

USNA-CS-TR-2011-02

December 22, 2011

Initial Report of the Dean's Cyber Warfare Ad Hoc Committee

August 21, 2009

updated November 25, 2009 by adding Table 1 and Figure 1

"In the past we have been protected from hostile attacks by broad oceans and friendly neighbors. Today, the evolution of cyber threats has changed the situation dramatically. In cyberspace, national borders are no longer relevant. Electrons don't stop to show passports. Potentially serious cyber attacks can be conceived and planned without detectable logistical preparation. They can be invisibly reconnoitered, clandestinely rehearsed, and then mounted in a manner of minutes or even seconds without revealing the identity and location of the attacker."

-- The Report of the President's Commission on Critical Infrastructure Protection, October 1997

"The architecture of the Nation's digital infrastructure, based largely upon the Internet, is not secure or resilient. Without major advances in the security of these systems or significant change in how they are constructed or operated, it is doubtful that the United States can protect itself from the growing threat of cybercrime and state-sponsored intrusions and operation...These and other risks have the potential to undermine the Nation's confidence in the information systems that underlie our economic and national security interests."

-- The Report of the President's 60-day Cyberspace Policy Review, May 2009

"We will accelerate and resource our cyberspace efforts—more skilled network operators, a robust global network infrastructure, and a force capable of continued operations while defending against cyber-attacks."

-- Chairman of the Joint Chiefs of Staff Guidance for 2008-2009

Executive Summary

The Department of Defense has substantially increased the emphasis and investment being made to better position the military to operate effectively in a cyber warfare environment. Among the more notable recent developments have been the establishment of a new Cyber Warfare Command (USCYBERCOM) at Fort Meade, the establishment of a new Navy Fleet Cyber Command, as well as the reorganization of the OPNAV staff, merging N2 and N6 into a new information-warfare-centric organization.

Clearly, future Naval Academy graduates will be expected to know more about cyber warfare than those we have graduated in the past. The Academic Dean and Provost tasked an ad hoc committee—the Cyber Warfare ad hoc Committee—to examine how USNA can best ensure that the officers we provide are able to operate effectively in a cyber warfare environment. More specifically, the Committee was tasked with determining how USNA can invest our midshipmen with the tools, techniques and talents necessary to face this new environment, and asked the committee to examine what impact these new developments should have on the baccalaureate education offered at USNA.

In reaching its findings, the Cyber Warfare ad hoc Committee analyzed how our sister service academies and civilian undergraduate institutions incorporate cyber warfare concepts into their curricula. The Committee also examined what educations and skills various graduate institutions consider necessary preparation for entry into cyber warfare related curricula at their institutions. The OPNAV and CMC staffs were asked for their perspectives on the education and training that our graduates should receive in order to help the Navy and Marine Corps in this area.

On Aug 12th, the Committee unanimously agreed on the following recommendations:

- **Recommendation 1**: Create a required computer science technical core course that addresses the technical foundations of Cyber Warfare.
- **Recommendation 2**: Attain institutional designation as a NSA/DHS National Center of Excellence in IA Education.
- **Recommendation 3**: Create an "Interdisciplinary Cyber Warfare Center" that will serve to enhance midshipmen education in cyber warfare.
- **Recommendation 4**: Create cyber-related electives from interested departments that build upon the core course, and infuse cyber-related topics into existing courses.
- **Recommendation 5**: Add cyber warfare to plebe pro-knowledge.

The Committee feels that implementing these recommendations is necessary in order to produce cyber-capable unrestricted line officers that meet the needs of the Navy at what we define as a 'Foundational Level'. Higher levels of engagement (Proficient and Dominant) are also considered in this report. It is estimated that attaining the Foundational Level recommendations would require the hiring of 10 FTEs (full-time equivalent) faculty members, and the dedicated use of four standard classrooms that already exist in Michelson Hall but are currently being used for Language Studies.

Table of Contents

I. Introduction and Tasking

A. A Nation Under Attack

The US military is actively engaged in conflicts in Iraq and Afghanistan. Another conflict is occurring behind the scenes, in *cyberspace*—i.e., in the collection of interconnected networks used for communications and information transport, including the Internet, telecommunication networks, computer systems and embedded processors. In fact, classified military and government networks come under attack tens of thousands of times each day.

The more famous attacks make the headlines:

- In late 2006, the military took note when hackers broke in and disabled the Naval War College's computer network.
- In October 2006, hackers planted malicious code into the water treatment facility used by the city of Harrisburg, Pa.
- In the spring of 2007, a cyber attack disabled the government and financial networks throughout the entire country of Estonia.
- In mid-2007, hackers broke in to several Pentagon computer networks, including the unclassified Pentagon email system used by Secretary of Defense Robert Gates.
- In 2008, Chinese hackers attacked the computers used by Congressman Frank Wolf of Virginia and Congressman Christopher Smith of New Jersey.
- In February 2009, the administrative computer server for the Federal Aviation Administration was hacked.
- In July of 2009, the U.S. Treasury Department, Secret Service, Federal Trade Commission and Transportation Department web sites were subjected to a "denial of service" attack and disabled to various degrees.
- In early August 2009, the popular social networking sites, Twitter and Facebook, suffered outages caused by a sophisticated hacker attack.

But these are only the more famous attacks. The government reported 12,986 direct cyber assaults on federal agencies in 2007, as well as 80,000 attacks on Department of Defense computer systems,[1] more than double the number in 2006.[2] In May 2009, the Pentagon informed the House Intelligence Committee that its systems are scanned or

attacked more than 300 million times per day.[3] Intelligence officials estimate losses from cyber attacks to be in the multiple billions of dollars.[4]
But much more than money is at stake. Some intelligence officials worry that cyber attackers could take control of a nuclear power plant via the Internet, or wipe out the data of a major financial institution.[5] Could an adversary attack and disable a critical military network in the midst of a conflict? Could an adversary manipulate information? General Kevin Chilton, Commander of US Strategic Command, paints a chilling picture: "Suppose I put out an order on my computer that says I want all my forces to go left, and when they receive it, it says 'Go right.' "[6] This is not a futuristic concern: the Chinese People's Liberation Army has established information-warfare units to develop viruses to attack computer networks.[7]

The US has been somewhat slow to respond to this emerging threat at a national level. Under the Bush administration, cyber security efforts were centered in the Department of Homeland Security, although efforts were also scattered over the Department of Defense, the FBI, the CIA, and the individual services. The Center for Strategic and International Studies assembled a bipartisan commission of technology experts in the summer of 2007 to examine the best way for the US to consolidate its cyber security efforts. The commission concluded that "America's failure to protect cyberspace is one of the most urgent national security problems facing the new administration," and further noted that the cyberspace battle is "a battle we are losing." [8] The commission recommended consolidating cyber security efforts under a White House official, and, in fact, President Obama announced in May 2009 the establishment of a new cyber-security office at the White House, whose chief will oversee all efforts by the government to protect computer networks (this position remains unfilled as of early August 2009).

But even a year ago, the need for enhanced emphasis on cyber security was very much evident. In 2008, President Bush issued an executive order creating the Comprehensive National Cyber Security Initiative, supported by $6 billion in funding for 2009. It is estimated that the US might spend $30 billion in cyber security initiatives over the next few years.

B. What is Cyber Warfare?

What precisely is meant by the term *cyber warfare*? Although everyone seems to have a gut feeling for what this term implies, the U.S. military seems to actively avoid the term in its bureaucratic documents. But, in light of the fact that terms such as *cyber security*, *cybercrime* and *cyber attack* have entered the common lexicon, we do not feel compelled to shun the term.

In its simplest definition, cyber warfare involves warfare in cyberspace. Such warfare encompasses the subjects of network security, information assurance, intelligence, cryptology and infrastructure protection, in both defensive and offensive contexts.

We propose two working definitions for cyber warfare. The first is to simply use the definition of "Information Operations" presented in SECNAV INSTRUCTION 3052.2 of 6 March 2009.

Proposed Definition of Cyber Warfare (1)

> Cyber Warfare is the integrated employment of the core capabilities of electronic warfare, computer network operations, psychological operations, military deception, and operations security, in concert with specified supporting and related capabilities, to influence, disrupt, corrupt or usurp adversarial human and automated decision making while protecting our own.

The term "computer network operations" contained within the above proposed definition is quite loaded, encompassing the notions of "*Computer Network Attack*," "*Computer Network Defense,*" and "*Computer Network Exploitation.*" These three terms are specifically defined in SECNAV INSTRUCTION 3052.2 as:

- **Computer Network Attack (CNA):** Actions taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves.
- **Computer Network Defense (CND):** Actions taken to protect, monitor, analyze, detect and respond to unauthorized activity within DoD information systems and computer networks.
- **Computer Network Exploitation (CNE):** Enabling operations and intelligence collection capabilities conducted through the use of computer networks to gather data from target or adversary automated information systems or networks.

We also propose a second working definition of cyber warfare. As expected, this definition is closely allied with the definition above, and is based on the definition of the term *cyber* (just "*cyber*" without the following word *warfare*) found in a working document provided by CNO N153 (Education).

Proposed Definition of Cyber Warfare (2)

Cyber warfare is an interdisciplinary domain that converges:

- Information Operations
  - Computer Network Exploitation
  - Computer Network Attack
  - Computer Network Defense
  - Electronic Warfare
- Information Assurance
  - Integrity and Non-repudiation
  - Confidentiality
  - Assured Information Sharing (Authentication)
  - Highly Available Enterprise
- Network Operations: The activities conducted to operate and defend networks

In the above definition, the term *Integrity* refers to the need to ensure that our information is protected from any unauthorized changes, such as modifications, deletions, insertions or replay. The term *Confidentiality* refers to protecting our information from unauthorized access. The term *Authentication* refers to the need to ensure that we are communicating with the intended party; i.e., we want to be sure that the person on the other end is who he says he is. The term *Availability* refers to the need to ensure that our information is available to authorized users.

Finally, we note that the Chairman of the Joint Chiefs of Staff recently (November 2008) directed all military services to use the following definition of "cyberspace operations":[9]

> ***Cyberspace operations***: The employment of cyber capabilities where the primary purpose is to achieve military objectives or effects in or through cyberspace. Such operations include computer network operations and activities to operate and defend the Global Information Grid.

Again, we choose to use the term *cyber warfare* as described above. Although one might argue over the precise terminology to use (and, in fact, the Committee has learned that the DoD bureaucracy has spent *years* trying to nail down this terminology), no one would take issue with the fact that the national security of the United States depends on the security of military computer networks, and the security of the information contained therein. Cyber warfare is now viewed as an existential threat to the nation. Former National Intelligence Director Michael McConnell termed cyber security "the soft underbelly of the country." [10] General James Cartwright told Congress that a "cyber attack could, in fact, be in the magnitude of a weapon of mass destruction." [11]

C. The Navy Takes Action

Last year, shortly after President Bush launched the Comprehensive National Cyber Security Initiative, the individual military services, and the Defense Department as a whole, took actions to indicate the seriousness of their concerns. In August of 2008, the CNO noted that "The security challenges confronting Navy information and information systems are multiplying rapidly.... The threats are becoming more sophisticated and diverse, and Navy systems are inherently more vulnerable to surreptitious access, user misuse, abuse and malicious attacks." [12] And just weeks ago, on June 23, 2009, the Pentagon established a new command, The U.S. Cyber Command (USCYBERCOM), headquartered at Fort Meade, that will oversee efforts to defend and protect the military's computers and computer networks, and develop offensive cyber-weapons. (The Department of Homeland Security will remain in charge of protecting civilian networks and the nation's critical infrastructure). USCYBERCOM will be launched in October 2009, and will be headed by the Director of the National Security Agency.

The Navy will stand up a new Fleet Cyber Command, FLTCYBERCOM, to provide naval component support to USCYBERCOM. FLTCYBERCOM's mission will be to "serve as central operational authority for networks, intelligence, cryptology, SIGINT, information operations, cyber, electronic warfare, and space"[13] and, as with USCYBERCOM, will be based at Fort Meade and will become operational in October, 2009. Several existing naval commands that currently support some of these functions—e.g., Naval Network Warfare Command (NAVNETWARCOM) and Navy Information Operations Command (NIOC)—will be brought under and integrated into the new FLTCYBERCOM. In conjunction with standing up this new command, the CNO will reorganize the OPNAV staff, bringing N2 (Director of Naval Intelligence) and N6 (Communication Networks) together.

The Navy is also examining its officer community management in light of the increased focus on cyber warfare. At present, the officer component of the Navy's cyber warfare workforce draws from three communities: *Information Warfare* (1610), *Information Professional* (1600) and *Intelligence* (1630). The Navy is considering the creation of a new *Cyber* Unrestricted Line designation.

D. What is the Naval Academy's Role?

In the past, The United States Naval Academy has supported graduates who are equipped with the basic skills needed to excel in warfare on the seas, in the air, and on land. But cyberspace, in the words of General Kevin Chilton, Commander of the US Strategic Command, is as much a domain as the traditional domains of air, land and sea.[14]

According to VADM Jack Dorsett, the Director of Naval Intelligence, the CNO "has gone all-in as he positions the Navy to play a dominant role in the information-intensive disciplines." VADM Dorsett goes on to say of the CNO that "his concept is for information management, intelligence, cyber, etc., to form the very foundation of our future Navy." [15]

Since USNA provides the backbone of newly commissioned officers to the Navy and Marine Corps—the Navy "hires" all of our graduates, and Naval Academy graduates make up the largest segment of technically educated officers entering commissioned naval service each year— it seems clear that future Naval Academy graduates will be expected to know more about cyber warfare, to include information assurance and network security, than those we have graduated in the past. **Simply put, if cyber, in the CNO's view, is to form the "the *very foundation of our future Navy,*" and if USNA officers form the *foundation of the Naval officer corps,* then USNA should endeavor to ensure that it is producing officers capable of operating in this new cyber warfare intensive environment.**

There are other indications that the Navy will soon come to depend on USNA to provide officers who are ready to contribute to their command's success in a cyber warfare environment. The Navy's Cyber Workforce Strategy stipulates that the Navy requires a workforce that "understands how to design, build and operate network warfighting capabilities and enabling capacities within the domain" of cyberspace as well as "conduct planning and execute operations within the domain" of cyberspace. But the Navy's Cyber Workforce Strategy Document notes with some alarm that:

> "Navy has no direct recruitment program that targets college students with IT/Network related degrees. Consequently, we are not shaping our recruitment efforts to attract those skills or focusing our efforts on undergraduate schools with strong network security programs. The time has come for the Navy to take advantage of the undergraduate talent pool majoring in Network and Information degrees, a pool which would have the technical expertise to fill those junior officer billets afloat responsible for Communications and/or Information Systems

> that today are often filled by officers that have no expertise... **USNA accession of officers into a common source community for cyber would enable leadership to better shape manpower plans for supported cyber missions**."

Among the recommended actions that the Navy should commit to, the Cyber Workforce Strategy Document includes:

> "**Beginning accessions for the Navy's Cyber community at USNA** and NROTC and establishing recruitment criteria for cyber-related degrees and academic quality."

This is indeed a real and pressing need. The Chairman of the Joint Chiefs of Staff, Admiral Michael Mullen, expressed his intent to "accelerate and resource our cyberspace efforts—more skilled network operators, a robust global network infrastructure, and a force capable of continued operations while defending against cyber-attacks." [16]

To address these issues, the Academic Dean and Provost, Dr. William Miller, tasked an ad hoc committee—the Cyber Warfare Committee—to examine how USNA can best ensure that the officers we provide are able to operate effectively in a cyber warfare environment. More specifically, the Cyber Warfare Committee was tasked with determining how USNA can invest our midshipmen with the tools, techniques and talents necessary to face this new environment, and asked the committee to examine what impact these new developments should have on the baccalaureate education offered at the Naval Academy.

These initial questions immediately raise subordinate questions and concerns. What modifications in learning objectives, curricula, teachers and possibly facilities would be needed to ensure that USNA commissions warriors who are ready to contribute to their command's success in a cyber warfare environment? While the Naval Academy's mission is not to educate cyber warfare *specialists*, what educational foundation must a newly commissioned officer possess to function effectively in this cyber-warfare environment? How should USNA instill this expertise, while still maintaining its status as a first-class undergraduate institution, and while maintaining the proper balance between theory and application?

II. Committee Organization and Methodology

The membership of the Dean's Cyber Warfare ad hoc Committee initially consisted of twelve members:

- A Committee Chair, appointed by the Academic Dean and Provost.
- Two members each from Divisions I, II, III and IV, appointed by the associated Division Directors.
- A representative from ITSD, appointed by the Deputy for Information Technology.
- A representative from the Office of the Deputy for Finance, appointed by the Academic Dean and Provost.
- A representative from the Public Works Office, appointed by the Public Works Officer.

These committee members were:

- Prof. Don Needham, Committee Chair
- LCDR Rory Berke, Political Science Department
- LT Garrettson Blight, Division of Professional Development
- LT Cameron Collier, Officer Development/LEL Department
- Mr. Lou Giannotti; Deputy for Information Technology
- CAPT Mark Hagerott; History Department
- Ms. Megan Owen, NAVFAC Washington, Public Works Department, Annapolis
- Ms. Sara Phillips, Office of the Deputy for Finance
- Asst Prof. Ryan Rakvic, Department of Electrical and Computer Engineering
- LCDR Greg Sakryd, Weapons and Systems Engineering Department
- CDR Patrick Vincent, Computer Science Department
- Asst Prof. Richard Witt, Physics Department

In order to ensure that additional stakeholders were aware of the Committee's activities, and in order to solicit input from individuals with pertinent areas of expertise, the Chair appointed six additional members.

- To ensure that the Committee's efforts remained in concert and alignment with the broader views of the Naval Academy as a whole, the Chair invited a representative from the Faculty Enhancement Center, as well as a member of the Faculty Senate, to join the Committee.

- To ensure that the Committee's efforts remained in concert with the Navy's warfighting needs, and were in alignment with OPNAV plans and programs for education and training, the Chair invited two representatives from the OPNAV N15 Staff (Total Force Training and Education Division) to join the Committee.
- Since the National Security Agency hires many cyber workers and conducts the *Centers of Academic Excellence in IA Education Program*, and since the Director of NSA will head the new USCYBERCOM, the Chair invited the Naval Academy's NSA Visiting Professor to join the Committee as well as the officer representative of USNA's Cyber Defense Exercise.

These auxiliary committee members were:

- LtCol Tom Augustine, Cyber Defense Exercise (CDX) officer representative
- Ms. Lisa Augustyn-Castro, OPNAV N152 (Training Branch)
- Assoc Prof. Ric Crabbe, Faculty Senate Ex-Officio
- Dr. Peter Gray; Faculty Enhancement Center
- Dr. Eric Harder, Visiting National Security Agency Professor
- Mr. Steve Muir, OPNAV N153 (Education Branch)
- LCDR Brian Stites, NSA HQ, IW-OCM

Each of the Committee's members solicited the viewpoints and expertise from their respective departments/centers/agencies in order to provide a full range of options and issues for the Committee to consider. The Committee met weekly.

The road map the Committee followed is presented on the following page.

Dean’s Cyber Warfare ad hoc Committee Road Map

Final Goal: Determine how USNA can better develop midshipmen to serve effectively in the Navy and Marine Corps operating in a cyber warfare environment.

1. Describe in detail what we mean by a Naval Academy graduate who is better prepared to contribute as an unrestricted line officer in a cyber warfare environment. This description must be based on our customer’s input: What qualities do the Navy and Marine Corps desire of USNA graduates in order that they may more effectively contribute in the cyber warfare environment they will join in the fleet?

2. In light of the qualities that the Navy and USMC desire in graduates, examine how USNA can better prepare our graduates to contribute effectively in the Navy and Marine Corps cyber warfare environment. Put another way: How can USNA invest our midshipmen with the tools, techniques and talents necessary to face the new challenges of cyber warfare?

3. Evaluate the current curriculum, faculty preparedness, and resources necessary to meet the requirements of the Navy and Marine Corps cyber warfare environment.

4. Propose and develop a plan of action to better prepare our graduates to effectively operate in the Navy and Marine Corps cyber warfare environment. Put another way: What modifications in learning objectives, curricula, teachers and possibly facilities would be needed to ensure that USNA commissions warriors who are ready to contribute to their command’s success in a cyber warfare environment?

5. Explore potential advantages in collocating related personnel and facility resources to achieve better synergy, or even establishing some form of Cyber Warfare Center at USNA. Could this space be used also for research with NSA or with other colleges?

6. What unique features are envisioned that might enhance our contributions to the Navy and Marine Corps cyber warfare efforts (e.g., a Network Defense Lab, a Secure Operating Systems Lab, a Sensor Network Lab, a Student Research Lab, a Biometrics Lab, a Digital Forensics Lab, a Cloud Computing Research Lab, etc.)

From the Committee's membership, the Chair appointed four subcommittees composed of members from different divisions and/or backgrounds where possible. Each sub-committee was tasked to explore a separate area deemed critical to the Committee's review of cyber warfare. The subcommittees were tasked as follows:

<u>Cohort Institutions subcommittee</u> chaired by *DIV II rep CDR Patrick Vincent with LtCol Tom Augustine and assisted by Ms. Sara Phillips.* This subcommittee analyzed how our sister service academies (USAFA and USMA) and prominent civilian undergraduate institutions that hold NSA/DHS National Center of Academic Excellence in IA Education status:

- Communicate that they have a need for cyber warfare capable graduates (student outcomes, learning objectives).
- Incorporate cyber warfare concepts into their curricula for <u>every</u> graduate (if any schools do this).
- Incorporate cyber warfare concepts into their curricula for <u>just some</u> of their graduates – to include which majors (computer science, computer engineering, political science, etc.).
- Identify what infrastructure (networks, computer labs, etc) is needed to directly support the cyber-related curricula?

<u>Graduate Institutions subcommittee</u> chaired by Div I rep Prof. Ryan Rakvic with *DIV I rep LCDR Greg Sakryd* and assisted by Prof Ric Crabbe. This subcommittee focused on determining what graduate institutions like NPS and AFIT, organizations like the National Defense University, and prominent civilian graduate institutions with relevant programs, consider as necessary preparation for entry into cyber warfare related curricula at their institutions.

<u>CNO/CMC & other Commands Liaison subcommittee</u> *chaired by Div IV rep* LT Garrettson Blight with Div II rep Prof Rich Witt and Div III rep CAPT Mark Hagerott and assisted by Ms. Lisa Augustyn-Castro and Mr Lou Giannotti. Ths subcommittee contacted OPNAV and Commandant of the Marine Corps (CMC) staff to determine what they think unrestricted line officers' (aviators, submariners, surface, USMC ground, etc) need (i.e., not just the information warfare (IW) or information professional (IP) communities). Specifically, they endeavored to determine what our graduates need to know to help the Navy and Marine Corps in this area, and what valuable contributions USNA might make.

Leveraging Mid-Atlantic Organizations subcommittee chaired by Div III rep CDR Rory Berke with Div IV rep LT Cam Collier/Assisted by Mr. Steve Muir; Dr. Eric Harder; Ms Megan Owen. This subcommittee explored how USNA's proximity and relationships with NSA and other organizations in the mid-Atlantic region can be leveraged (e.g., faculty lend/lease opportunities, shared facilities and research opportunities).

III. Alignment with USNA 2020 Vision, Graduate Attributes and USNA Strategic Imperatives

The Naval Academy continually adapts its academic program to satisfy the relevant Navy and Marine Corps needs that are expected to arise over the next decade. Indeed, it is important that the curriculum be adjusted as necessary to ensure midshipmen are prepared academically for the challenges they will face in the early years of their military service as officers in the 21st century Navy and Marine Corps.

In response to a changing world, and in order to continually improve USNA as a premier leadership organization, USNA has developed a comprehensive Strategic Vision (The 2020 Vision[17]) to guide the institution's future actions and ensure that the needs of the Navy and Marine Corps are continuously met. Additionally, the Naval Academy has defined Strategic Imperatives and Graduate Attributes to support the 2020 Vision.

The USNA 2020 Vision is:

> ***To be the nation's premier institution for developing future naval leaders from diverse backgrounds to serve in an increasingly interdependent and dynamic world.***

The USNA 2020 Vision is attained through the recognition and development of "attributes" desired of graduates, and these attributes are reinforced and strengthened through the implementation of "strategic imperatives."

In this section of the report, we show how the efforts to better develop midshipmen that can serve effectively in the Navy and Marine Corps operating in a cyber warfare environment aligns with the USNA Graduate Attributes and the USNA Strategic Imperatives.

A. USNA Graduate Attributes

The seven USNA Graduate Attributes are:

- Selfless. Selfless leaders who value diversity and create an ethical command climate through their example of personal integrity and moral courage.

- Inspirational. Mentally resilient and physically fit officers who inspire their team to accomplish the most challenging missions and are prepared to lead in combat

- Proficient. Technically and academically proficient professionals with a commitment to continual learning.

- Innovative. Critical thinkers and creative decision makers with a bias for action.

- Articulate. Effective communicators.

- Adaptable. Adaptable individuals who understand and appreciate global and cross-cultural dynamics.

- Professional. Role models dedicated to the profession of arms, the traditions and values of the Naval Service and the constitutional foundation of the United States.

The effort to better develop midshipmen to serve effectively in the Navy and Marine Corps operating in a cyber warfare environment aligns with two of the USNA Graduate Attributes:

- **Proficient**. Technically and academically proficient professionals with a commitment to continual learning.

  As noted the CJCS National Military Strategy for Cyberspace Operations (NMS-CO)[18] : "DoD personnel operating in cyberspace must have a thorough understanding of the rapidly evolving procedural and technical mechanisms required to conduct cyberspace operations."

- **Innovative**. Critical thinkers and creative decision makers with a bias for action.

  As noted the CJCS National Military Strategy for Cyberspace Operations (NMS-C)) a key feature of cyberspace is technical innovation. Quoting from this report: "Cyberspace evolves to ongoing technical innovation and is the only domain whose underlying structure can be dynamically reconfigured... Keeping pace with technological change requires sustained and constant vigilance and high degrees of domain expertise."

B. USNA Strategic Imperatives

The nine USNA Strategic Imperatives are:

1. Recruit, admit and retain a diverse and talented Brigade of Midshipmen.

2. Graduate officers whose attributes and educational and experiential preparation meet the Navy and Marine Corps' current and future requirements.

3. Attract, develop, and retain faculty and staff—both civilians and military—who model the highest academic, professional, and ethical standards.

4. Integrate all midshipmen's moral, mental, and physical core experiences to prepare them for future service in any naval warfare community.

5. Align ethical leadership and character development efforts across all academic, professional, athletic and extracurricular programs.

6. Leverage internal and external collaborations to engage midshipmen in relevant learning opportunities that develop the broad range of competencies required by the 21st century Naval Service.

7. Establish and maintain state-of-the-art facilities that inspire and support the pursuit of excellence.

8. Apply exemplary business and assessment practices that ensure the sound stewardship of Academy resources and result in continual process and program improvement.

9. Develop strategic relationships with alumni, friends and national and international institutions of influence that contribute to the Naval Academy's success and America's security and prosperity.

The effort to better develop midshipmen to serve effectively in the Navy and Marine Corps operating in a cyber warfare environment aligns with the following Strategic Imperatives taken from the full list above. We underline and italicize the appropriate section of text, and then elaborate for each.

Strategic Imperative 2. Graduate officers whose attributes and educational and experiential preparation meet the Navy and Marine Corps' current and *future requirements*.

> Clearly, officers in the future will require an enhanced knowledge of cyber warfare. The National Military Strategy for Cyberspace Operations (NMS-CO) notes that "creating and developing the force necessary to conduct cyberspace operations applies to people, describing the need to ensure personnel receive adequate, consistent training and the tools necessary to accomplish mission objectives.... This capability ensures the necessary forces to implement Information Operations and network operations are prepared to conduct operations."
>
> The NMS-CO notes that "Absent significant effort, the United States will not continue to possess an advantage in cyberspace... Unlike other warfighting domains, the United States risks parity with adversaries (in cyberspace)." The document goes on to list as a priority the need for "Tailoring education and training to meet specific needs of leaders, professionals and users in cyberspace."

Strategic Imperative 4. Integrate all midshipmen's moral, mental, and physical core experiences to prepare them for *future service in any naval warfare community*.

> The 2004 National Military Strategy noted that "The Armed Forces must have the ability to operate across the air, land, maritime space and cyberspace domains of the battlespace." The CNO's concept is for "information management, intelligence, cyber, etc., to form the very foundation of our future Navy."
>
> In 2008, the CNO's Strategic Studies Group (SSG) recommended as one of three "overarching actions" that the Navy establish an Unrestricted Line Cyber Warfare Community, and, more generally, recommended that the Navy enhance cyber warrior education and training. The 2008 CNO SSG also recommended that the Navy develop a training strategy to improve cyber awareness and the ability of every member of the Navy to be cyber-enabled. Training should be delivered through a variety of methods, including accession training.
>
> The Navy's Cyber Workforce Strategy stipulates that the Navy requires a workforce that "understands how to design, build and operate network warfighting capabilities and enabling capacities within the domain" of cyberspace as well as "conduct planning and execute operations within the domain" of

cyberspace and notes that USNA accession of officers into a common source community for cyber would enable leadership to better shape manpower plans for supported cyber missions.

Strategic Imperative 6. Leverage internal and *external collaborations* to engage midshipmen in relevant learning opportunities that develop the broad range of *competencies required by the 21st century Naval Service*.

USNA should explore the possibility of midshipmen collaborating with cyber warfare organizations, specifically with the new FLTCYBERCOM and USCYBERCOM commands. Arrangements for summer internships with the National Security Agency, the Naval Warfare Development Command and the Naval Research Lab are already in place, and should be expanded. USNA should collaborate with USMA and USAFA in cyber warfare exercises and operations.

IV. Examination of Practices of Cohort Institutions

Many colleges and universities have already moved forward with innovative well-developed cyber warfare curricula (although the term *cyber warfare* is never explicitly employed; see the discussion in Chapter 1). In an effort to determine the best path forward for USNA, the Committee analyzed how our sister service academies (USAFA and USMA) and prominent civilian undergraduate institutions that hold NSA/DHS National Center of Academic Excellence in IA Education status:

- Communicate that they have a need for cyber warfare capable graduates (student outcomes, learning objectives).

- Incorporate cyber warfare concepts into their curricula for <u>every</u> graduate

- Incorporate cyber warfare concepts into their curricula for <u>just some</u> of their graduates – to include which majors (computer science, computer engineering, political science, etc.).

- Identify what infrastructure (networks, computer labs, etc) is needed to directly support the cyber-related curricula?

A. <u>Past Practices at USNA</u>

In order to determine the best path forward, it was deemed helpful to first determine where we, as an institution, are now, and where we have been in the past with respect to incorporating cyber warfare concepts into the USNA curriculum. Each USNA academic department was asked to examine their last five years of course offerings in order to answer the question: “What cyber warfare related courses are currently taught, or have been previously taught, by your Department?”

Although several USNA course offerings glancingly touch upon topics that fall under the cyber warfare umbrella, there are several courses that directly treat of cyber warfare (as broadly defined). For example, each midshipman majoring in Information Technology is required to take the introductory information assurance course (IT430), and may also take the advanced information assurance course (IT432) as an elective. Students majoring in Computer Science may also take these two information assurance courses as major electives. The Electrical and Computer Engineering Department regularly offers an elective course in biometrics. The Computer Science Department and the Physics

Department have recently offered elective courses in cryptography and quantum cryptography, respectively, and the Computer Science Department also recently ran an elective course in Computer Forensics. The Political Science Department has started to address cyber warfare topics into a number of elective offerings.

A full list of all past and present cyber-related course offerings is presented in Appendix A, along with a brief description that focuses on the cyber warfare aspects of each course, typical enrollments, the intended audience, any infrastructure requirements, and any issues relating to the periodicity of the offering.

The Committee originally intended to survey the following six schools for examination of their undergraduate programs:

1. The United States Air Force Academy (USAFA)
2. The United States Military Academy (USMA)
3. The University of Tulsa
4. Mississippi State University
5. The Johns Hopkins University (JHU)
6. Capitol College

The Committee subsequently learned that all relevant initiatives at the JHU (e.g., information assurance, network defense, etc.) are entirely directed toward graduate students. JHU is thus discussed in Chapter V: Examination of Practices of Graduate Institutions. Capitol College, originally chosen based on the reputation of the College’s Vice President, Dr. Vic Maconachy (a nationally renowned authority in the field of information assurance), was also dropped from consideration because the college’s student body is so small and unrepresentative of USNA (the entire college—all majors—produced 51 bachelor’s degrees in all 2007).

Thus, the Committee limited its examination to USAFA, USMA, University of Tulsa and Mississippi State University. The cyber warfare-related programs at these institutions are discussed in turn. The general template of baseline questions as ked of the institutions is provided in Appendix B.

B. Cyber Education at the U.S. Air Force Academy

B.1. Overview

The cyber education efforts at the United States Air Force Academy are centered in the *Academy Center for Cyberspace Research* (ACCR). The ACCR, started in 2004, is housed in the Computer Science Department. Founded to enhance cadet education and faculty development through cutting-edge computer security research, the ACCR is staffed by a Director, two Research Assistants and one lab technician. The ACCR in the past has also hosted visiting researchers. The ACCR maintains a strong relationship with NSA, and the Air Force Academy hosts a Visiting NSA Professor who conducts research, teaches, assists in curriculum development and promotes awareness in information assurance and cyber-related topics.

The stated mission of the ACCR is "to enhance cadet education through research in the domain of cyberspace."

The ACCR serves as a focal point for cyber education at the Air Force Academy. The ACCR assists in Information Assurance-related curriculum development and instruction, conducts and encourages research with students and faculty (both in-house and in support of outside sponsoring agencies), and increases cyber awareness across the student body through a host of innovative activities (described in more detail later). The ACCR receives approximately $500,000 each year in external funding from various agencies.

B.2 Certification

Since 2005, the United States Air Force Academy has been designated a NSA/DHS National Center of Academic Excellence in IA Education, and elected to pursue re-certification in 2008. Certifications are now good for 5 years.

B.3. Infrastructure

There are two labs associated with the ACCR: an Information Warfare Lab (used in the Information Warfare class and for general research) and the Network Defense Lab (used for the annual Cyber Defense Exercise). These two labs are entirely dedicated to cyber-warfare courses, exercises and research.

B.4. Cyber Education

We next summarize what the ACCR does:

- For all students at the Air Force Academy
- For many students at the Air Force Academy, but not all
- For a small select group of specialized students
- For cyber education in general

What does the ACCR do for all students?

The Air Force Academy provides a three-credit lecture course, *Introduction to Computer Science*, taken by all students in their first year. Approximately 50% of the material in this course is centered on cyber-related topics (the remainder of the course is dedicated to algorithmic thinking and logical problem solving). Although the course is formally annotated as a three-credit "lecture" course, the class actually contains numerous integrated hands-on exercises, requiring that the students use their laptops. The ACCR provides a substantial amount of material for this course, and the Computer Science faculty continuously monitor the course to ensure it remains relevant and up-to-date.

What does the ACCR do for many students?

Initiative 1: Infusing Cyber Topics Across the Curriculum. The ACCR has integrated cyber related topics throughout many courses across the Air Force Academy (e.g., *Communications Systems* in the Electrical Engineering Department, *Politics and Intelligence* in the Political Science Department, *Special Operations* in the Military Strategic Studies Department). Most notably, the ACCR recently facilitated a special course in *Cyber Law* taught by the Law Department. In general, the ACCR continually (though informally) contacts other academic departments and suggests cyber-related topics that might be applicable to the curriculum.

Initiative 2: Cyber Warfare Cadet Club. Last fall, the ACCR founded the Cyber Warfare Cadet Club, which now meets regularly. The Club is open to any student who simply has an interest in cyber related topics. Participation from non-CS majors is highly encouraged; there are no prerequisites aside from the *Introduction to Computer Science* freshman year course required of all students.

The Cyber Warfare Cadet Club, which now has approximately 40 members from various majors, hosts guest lectures on cyber related topics, practices hands-on network defense and network attack operations, and runs competitions among their members.

Initiative 3: Summer Information Operations Program. This summer, the ACCR piloted a *Summer Information Operations Program* intended to expose 20 non-CS majors to the concepts of Information Warfare. This program, run by two faculty members and one Research Assistant, included lectures, labs and hands-on activities. The students were tasked to plan and execute an information operation against another group. The long-range goal is that this initiative will target 120-150 cadets per year.

Initiative 4: Cyber Warfare Testbed. In the new academic year, the ACCR is planning to install an isolated "Cyber Warfare Testbed," which will be an extensive isolated network used to run advanced cyber-related tests and exercises, to include such advanced topics as creation and control of botnets.

Initiative 5: Guest Lecture Program. The ACCR invites distinguished guest lecturers to the Air Force Academy for presentations open to all students and faculty.

What does the ACCR do for some select students?

The Air Force Academy provides three classes designated as "Information Warfare" classes (*Cryptography*, *Information Warfare* and *Network Defense*), all housed within the Computer Science Department. Most students who take these courses are CS majors, although the occasional engineering student is present. These three courses constitute a designated "cyber warfare track," and students who take all three receive an Information Warfare track notation on their transcript. The Computer Science department has graduated over 50 majors with this cyber warfare emphasis.

The Computer Science Department's Network Defense course culminates with the annual NSA sponsored Computer Defense Exercise (CDX). In the nine years that the CDX has been conducted, the Air Force Academy has won the competition twice and finished second four times.

The ACCR has also integrated cyber related topics throughout many courses in the Computer Science curriculum (e.g., Computer Networks).

The ACCR facilitates research between students and agencies (primarily NSA, but others as well) in conducting cyber-related summer research. The ACCR serves as the focus of CS Department research (the ACCR Director is the CS Department's Research Director as well), offering and facilitating independent cyber-related research topics and projects for interested students and faculty.

The ACCR supports faculty travel to conferences and training.

What does the ACCR do for cyber education in general?

The ACCR facilitates the annual Front-Range Security Conference. The Air Force Academy was a founding member of the Front Range Information Security Colloquium (FRISC) which hosts this annual meeting of schools to share educational and research experiences in information assurance. The goal is to establish a community of educators and researchers in the area and establish a forum for exploring collaborations in information security-related research and education.

The ACCR facilitates an annual Computer and Network Vulnerability Assessment Simulation (CANVAS). This is a competitive exercise to assess security vulnerabilities in a complex computer system that was cooperatively founded and developed with Colorado State University (CSU) in 2006. The exercise typically includes 60 students and 10 faculty members from 5 Front Range schools with support from NSA

The ACCR collaborates with AFIT and USMA on cyber-related concerns.

The ACCR is an active participant in the annual Colloquium for Information Systems Security Education.

Several members from the Computer Science Department faculty, in collaboration with AFIT, assist the Air Force in defining the cyber-related career field training requirements.

B.5. Summary

The Air Force Academy has an outstanding program that instills cyber knowledge, skills and abilities into the student body as a whole, and in core groups of students in particular. Starting with USAFA's required computer science technical core course that addresses the technical foundations of Cyber Warfare, which is then built upon in upper level courses, their efforts in this area far surpass anything currently present at the Naval Academy. The Air Force Academy's ACCR provides a template that USNA would be wise to emulate.

C. Cyber Education at the U.S. Military Academy

C.1 Overview

The cyber education efforts at the United States Military Academy are centered in the *Information Technology and Operations Center* (ITOC). The ITOC, started 20 years ago (with an original focus on Artificial Intelligence), is housed in the Electrical Engineering and Computer Science Department. Since 1999 the ITOC has had a vision of "an internationally recognized center of excellence in education, research and development in information technology and information operations." The ITOC is staffed by a Director (Military PMP), two researchers (Military PMPs), one half-time Military PMP from Computer Science, one systems analyst and one administrator. The ITOC maintains a strong relationship with NSA, and the Military Academy hosts a Visiting NSA Professor who conducts research, teaches, assists in curriculum development and promotes awareness in information assurance and cyber-related topics.

The ITOC serves as a focal point for cyber education at the U.S. Military Academy. ITOC is "dedicated to researching and teaching information assurance, computer and network security. The mission of ITOC is "to educate and inspire cadets and faculty in the acquisition, use, management, and protection of information through innovative teaching, curriculum development, research and outreach to Army, DoD and federal agencies." The ITOC assists in Information Assurance-related curriculum development and instruction, conducts and encourages research with students and faculty (both in-house and in support of outside sponsoring agencies), and increases cyber awareness across the student body through a host of innovative activities (described in more detail later).

C.2. Certification

Since 2001, the United States Military Academy has been designated a NSA/DHS National Center of Academic Excellence in IA Education and elected to pursue re-certification, in 2004, and will likely recertify this year (2009).

C.3. Infrastructure

The United States Military Academy has a very large infrastructure associated with the EECS Department and the ITOC. The ITOC maintains two labs including the Multipurpose Computing lab open to many students working on cadet capstone and independent study projects, and the Information Warfare and Analysis Lab designed to allow cadets to test their IA skills in defending a network. In addition to these labs, the EECS Department maintains about 12 classrooms, with rolling racks of network equipment used by the Plebe and Junior core classes.

C.4. Cyber Education

We next summarize what the US Military Academy does with regard to cyber education:

- For all students at the U.S. Military Academy
- For many students at the U.S. Military Academy, but not all
- For a small select group of specialized students
- For cyber education in general

What does the USMA do for all students with regard to cyber education?

The U.S. Military Academy provides a three-credit lecture course, *IT105: Introduction to Computing and Information,* taken by all students in their first year, stressing problem-solving using information technology and computers including use of programming and robotics. Most lectures contain an integrated hands-on component. The ITOC provides a substantial amount of material for this course, and the Computer Science faculty members continuously monitor the course to ensure it remains relevant and up-to-date.

What does the USMA do for many students in terms of cyber education?

Initiative 1: IT305, Information Technology for Military Applications is required by all majors except "ABET accredited majors." In USNA-lingo, this course is required for all Division II and Division III majors.

Initiative 2: Cadet Special Interest Group in Security, Audit and Control (SIGSAC). This organization is open to all majors, as an after school activity. Although the SIGSAC is chartered under the student ACM Chapter, SIGSAC emphasizes that members need not be Computer Science majors, and that the club has members in all disciplines including those majoring in foreign languages, social sciences, math, and chemistry. The SIGSAC is focused on Cyber Warfare and organizes monthly guest speakers, monthly programming contests, multiple mini-exercises and the annual Cyber Defense Exercise. Most of the 50 person EECS department faculty are very involved, and they invite faculty from other majors to support this endeavor as well.

Initiative 3: Incorporation of Research Centers into Year long capstone projects. Most students in Engineering and Sciences are required to complete a year-long capstone projects. The ITOC arranges funding and real-world customers so that students can help solve a real-world problem and present their capstones to audiences outside the Academy. The ITOC currently holds collaborative relationships with more than a dozen federal agencies.

Initiative 4: Funding of Cyber-Security related projects and research. The ITOC arranges funding with 6-10 major grant proposals / funding opportunities per year. This funding is used to support much of the Computer Science and Electrical Engineering faculty and student research, as well as their equipment and travel needs. These grants also fund dozens of summer-long student internships to various government agencies. In order to do this, the ITOC fully engages and maintains strong working relationships with numerous government agencies.

What does the ITOC do for some select students?

In addition to the two required information technology courses of most majors, The U.S. Military Academy provides to its CS/EE, math, and some Social Science majors five classes directly relating to “Information Assurance, Information

Warfare and Forensics " (*Forensics*, *Cryptography (Math), Policy for Cyber Warfare (EE/CS/Social Sciences), Network Administration, and Information Assurance*. Additionally, the Software Systems Design I & II and IT Integrative Capstone I & II are strongly focused on Cyber Defense.

The Computer Science Department's Information Assurance course culminates with the NSA sponsored Computer Defense Exercise (CDX). The U.S. Military Academy has won this competition five times in the exercise's nine year history, and has won the exercise the past three years in a row.

The ITOC has also integrated cyber related topics throughout many courses in the Computer Science curriculum (e.g., Computer Networks).

What does the ITOC do for cyber education in general?

The ITOC facilitates research between students and agencies in conducting cyber-related summer research.

The ITOC supports faculty and student travel to conferences and training.

C.5. <u>Summary</u>

The U.S. Military Academy has an outstanding program that instills cyber knowledge, skills and abilities into the student body as a whole, and in core groups of students in particular. Starting with USMA's required computer science technical core course that addresses the technical foundations of Cyber Warfare, which is then built upon in upper level courses including a second computer science technical core course required of all non-ABET accredited majors, their efforts in this area far surpass anything currently present at the Naval Academy. The U.S. Military Academy's ITOC provides a template that USNA could implement in parts, but would require an enormous faculty and student focus and dedication to cyber-security related subjects in order to mirror their level of success.

Table 1 provides a summary of the current cyber-related academic exposure given to cadets and midshipmen at USMA, USNA, and USAFA.

Table 1 Summary of current cyber exposure at USMA, USNA, and USAFA.

	USMA	USNA	USAFA
Required CS Cyber Core Course(s) for all	- 3 cr (IT105) for all + - 4 cr (IT305) for all non-ABET majors - Taught by CS dept	no	- 3 cr (CS110) for all - Taught by CS dept
Cyber Warfare Center	Info Tech and Ops Ctr Staff: 3.5 FTEs, plus 1 sys admin, 1 office staff	no	Academy Center for Cyberspace Research Staff: 2 FTEs, plus 1 sys admin
Annual CDX	yes	yes	yes
Cyber Warfare Club	yes	no	yes
NSA/DHS CAE IA Education	Institutional designation since 2001	no	Institutional designation since 2003

D. Cyber Education at the University of Tulsa

D.1 Overview

The cyber education efforts at the University of Tulsa are centered in the *Institute for Information Security* (iSec). The iSec, started 13 years ago as the Center for Information Security, was recast in 2007 to expand its focus to include relationships with companies in the private sector. The iSec is housed in the College of Engineering and Natural Sciences.

The iSec is staffed by a Director who is on the Computer Science faculty, and has a core group of seven faculty members. The iSec has alliances with seven additional faculty members who are more loosely affiliated.

The mission of the iSec is to support a multi-disciplinary program of study and research tackling cyber security issues on a global scale, to support research in such areas as critical infrastructure protection, security engineering, enterprise security and digital forensics and to help establish Tulsa as a hotbed for information security research and development.

More specifically, as iSec relates to undergraduates, its primary goals are threefold. First, iSec seeks to educate and prepare students for the cyber-related civilian workforce. Second, iSec conducts and facilitates research in cyber security. Third, iSec facilitates cyber-related service opportunities, such as performing risk assessments for companies and setting up firewalls for nonprofit organizations.

Although iSec is not formally under the cognizance of any academic department, a majority of the students affiliated with the institute are Computer Science majors. At any given time, approximately 30-40 undergraduate CS majors (as well as 30 graduate students) are conducting cyber-related research through the iSec. At any time, approximately 120 students are taking classes associated with iSec (approximately 80 CS majors, with the remainder from a diverse mix of disciplines including business and law).

D.2 Certification

Since 2001, the University of Tulsa has been designated a NSA/DHS National Center of Academic Excellence in IA Education.

D.3 Infrastructure

There are six labs associated with the iSec supporting classes, research and graduate student workspaces. The iSec has no dedicated classrooms.

D.4. Cyber Education

We next summarize what the iSec does:

- For all students at the University of Tulsa
- For many students at the University of Tulsa, but not all
- For a small select group of specialized students
- For cyber education in general

What does the iSec do for all students?

The University of Tulsa does not provide a course centered around cyber-related topics for all students.

What does the iSec do for many students?

The University of Tulsa does not provide broad educational or research outreach programs to a wide swath of the student body.

What does the iSec do for some select students?

The size of the student body at the University of Tulsa is approximately 3100 undergraduate students. Since only 120 students are affiliated with iSec, and all of these students are self-selected, and most of these students are Computer Science majors, we deem all of iSec's efforts to be directed to a "select" group of students.

The iSec maintains the University of Tulsa's rigorous information assurance curriculum, with the chief goal of producing exceptional graduates who will make significant contributions as professionals and leaders in the field. The iSec contributes to nine separate CS courses: (1) Computer Security, (2) Information System Security Engineering, (3) Risk Management for Information Systems, (4) Secure Electronic Commerce, (5) Information System Assurance, (6) Enterprise Security Management, (7) Network Security, (8) Computer and Network Forensics, and (9) Secure System Administration and Certification.

The iSec also oversees a novel interdisciplinary program, recently facilitating courses conducted by the History, Law, Political Science and Economics Departments, under such varied titles as Politics of Cyber Terrorism, Cyber Law and Policy, and National Security Law.
Perhaps most interesting, iSec has designed an Information Security Certificate Program patterned after the various information security training levels established by the Committee on National Security Systems (CNSS) Standards. There are five CNSS standards for information assurance education, and University of Tulsa's iSec curriculum was the first to be certified under all five standards. In fact, iSec specifically developed several courses around these national standards.

To receive a certificate in a designated category, students must complete a specific set of courses. For example, students who complete the Computer Security course, two system courses and a fourth IA elective course receive a certificate stating that they have satisfied all requirements for the CNSS 4011 (Information Security Personnel). Basically, the program certifies that students satisfying program requirements are trained to the federal standards for information systems security professionals.

While the University does not grant minors or other such designations, these certificates provide graduates a means of ensuring employers recognize their coursework in cyber security.   These certificates are the only credential that recognizes a student's participation with the iSec.

The iSec hosts students participating in the Cyber Corps Program. This program provides students with a stipend of approximately $1,000 per month, and pays all tuition for two years, room and board, and travel to conferences.   Students complete a summer internship in a federal agency, and by the end of the second year earn a degree in computer science in addition to multiple federal-level computer security certificates as endorsed by the Committee on National Security Systems (CNSS) (discussed above).   Students participating in the program must serve at a Federal agency in an information assurance position for a period equivalent to the length of the scholarship or one year, whichever is longer. The vast majority of these students go to NSA.

What does the iSec do for cyber education in general?

The iSec has formed research partnerships with private industry, focusing on such topics as extracting evidence from electronic devices and analyzing vulnerabilities in control systems for power industries.

The iSec has formed research partnerships with several government agencies, including the Memorial Institute for the Prevention of Terrorism in Oklahoma City and the Institute for Security Technology Studies at Dartmouth College.

The iSec retains contact with the Critical Infrastructure Protection Working Group and the Digital Forensics Working Group.

The iSec has hosted meetings of the "Cyber Corps."

D.5 Summary

The University of Tulsa has an outstanding program that instills cyber knowledge, skills and abilities into a core groups of students.

E. Cyber Education at the Mississippi State University

E.1 Overview

The cyber education efforts at the Mississippi State University are centered in the *Center for Computer Security Research* (CCSR). The CCSR is dedicated to the scientific exploration of computer vulnerabilities with the objective of improving prevention and detection techniques through several core research areas. The CCSR was established in 2001 within the Department of Computer Science and Engineering, and is now recognized as a multidisciplinary Center within the College of Engineering.

The *mission* of the CCSR, as stated on its website, is "to serve as a focus organization for collaborative work with faculty and students from multiple colleges at MSU in the area of computer security and information assurance." The research activities of the CCSR include intrusion detection in high performance computing systems, homeland security initiatives, computer forensics, management of secure information systems, criminal justice issues in cyber crime, and cyber policy and procedure.

The CCSR works to promote cross-disciplinary research and research proposals, facilitates collaborations with other academic institutions and industry, and supports the law enforcement community. The CCSR is staffed by a Director who is on the Computer Science faculty (presently the Chair of the Computer Science Department), and has a core group of fourteen faculty members. It is interesting to note that 10 of the 18 tenured/tenure track faculty in the Computer Science Department do work wit the CCSR.

E.2 Certification

Since 2001, the Mississippi State University has been designated a NSA/DHS National Center of Academic Excellence in IA Education. The designation was renewed in 2004 and 2007.

E.3 <u>Infrastructure</u>

There are five labs associated with the CCSR: a Forensics Teaching Lab, an IA Teaching Lab, an IA Research Lab, a Business Information Systems Security Lab and a Supervisory Control and Data Acquisition (SCADA) Lab. The CCSR received $4.5 million in funding in 2008.

E4. <u>Cyber Education</u>

We next summarize what the CCSR does:

- For all students at Mississippi State University
- For many students at Mississippi State University, but not all
- For a small select group of specialized students
- For cyber education in general

What does the CCSR do for all students?

The CCSR does not provide a course on cyber-related topics for all students.

What does the CCSR do for many students?

The CCSR does not provide broad educational or research outreach programs to a wide swath of the student body. Most of the students involved with the CCSR are Computer Science majors or Engineering majors.

What does the CCSR do for some select students?

As with the University of Tulsa, the CCSR has designed an Information Assurance Professional Certificate Program patterned after the various information security training levels established by the Committee on National Security Systems (CNSS) Standards.

To receive the CCSR Information Assurance Professional Certificate, students must complete a specific set of courses totaling to a minimum of 15 semester hours. Students must complete courses in Information and Computer Security, Computer Crime and Forensics and Network Security and Cryptography, and then must select two courses from a list of seven electives. Basically, the program certifies that students satisfying program requirements are trained to the federal standards for information systems security professionals.

Mississippi State University organized a major forensics training center in 2005 in concert with the National Forensics Training Center, which was funded by the Department of Justice to train law enforcement officers to fight cyber crime. There are two primary facilities for the National Forensics Training Center, one of which is on the campus of Mississippi State University. These facilities provide students with hands on experience with some of the latest tools and equipment in digital forensics.

The CCSR organized a Supervisory Control and Data Acquisition (SCADA) Lab in 2007 that has already played a major role in discovering serious flaws in SCADA user-interface software and thwarted a Distributed Denial of Service Attack planned for July 4, 2009.

What does the CCSR do for cyber education in general?

The National Forensics Training Center at Mississippi State University offers courses free of charge to for all law enforcement personnel (e.g., police officers, state troopers), in order to prepare them to conduct digital investigations.

CCSR has recently extended the law enforcement training that is offered by the National Forensics Training Center at Mississippi State University to veterans as well. Funded by the National Science Foundation, this effort provides vocational training at no charge for veterans, including those in transition and/or disabled.

The CCSR hosts students participating in the Cyber Corps Program. This program provides students with a stipend of approximately $1,000 per month, and pays all tuition for two years, room and board, and travel to conferences. Students complete a summer internship in a federal agency, and by the end of the second year earn a degree in computer science. Students participating in the program must serve at a Federal agency in an information assurance position for a period equivalent to the length of the scholarship or one year, whichever is longer. The vast majority of these students go to NSA.

E.5 <u>Summary</u>

Mississippi State University has an outstanding program that instills cyber knowledge, skills and abilities into a core group of students.

V. Examination of Practices of Graduate Institutions

In an effort to determine what should be accomplished at the undergraduate level, the Committee decided to examine what *graduate* institutions like NPS and AFIT, organizations like the National Defense University, and prominent civilian graduate institutions with relevant programs, consider as necessary preparation for entry into cyber warfare related graduate curricula at their institutions?

A number of graduate institutions were canvassed to determine what skill sets were necessary for entry into cyber warfare related curricula. Given the wide range of graduate institutions and objectives, institutions were divided into 3 distinct groups: civilian institutions, academic military institutions and professional military institutions.

A. <u>Civilian Institutions</u>

A representative cross-section of civilian institutions with cyber warfare related graduate programs were reviewed. Selection was based on military affiliation and informal rankings. Because the term "cyber warfare" is not commonly used outside DoD organizations, programs in information assurance, cyber security, and related fields were considered.

The following institutions were reviewed:

1. *MIT* focuses predominantly on theoretical research experiences.

2. *Mississippi State University* – desires students with science and engineering backgrounds and strong problem solving skills. They "can teach the computer security skill."

3. *Tulsa* – desirable for students to take a course in "Introduction to Computer Security," but most students are "foundational."

4. *Johns Hopkins University* maintains strong ties with the DoD through their Applied Physics Lab (APL). John's Hopkins' programs focus on theoretical research with APL funded projects with DoD applications.

5. *Purdue University*'s program is math based, emphasizing cryptography and security.

B. Academic Military Institutions

The Navy and Air Force maintain dedicated graduate education institution in Monterey, California and Dayton, Ohio respectively. The Army does not maintain a dedicated graduate institution, but has agreements with both NPS and AFIT to provide graduate education to Army personnel. Both NPS and AFIT focus on developing the technical expertise of their graduates for application within specific military career fields.

B.1. Naval Post Graduate School (NPS).

The mission of NPS is to provide relevant and unique advanced education and research programs in order to increase the combat effectiveness of U.S. and Allied armed forces and enhance the security of the United States. In support of this mission, NPS provides masters and doctoral degrees as well as multiple certificates in Information Assurance. While these programs support the Information Professional (IP) Community, the enrollment of officers from this community has been severely limited.

B.2. The Air Force Institute of Technology (AFIT).

The mission of AFIT is to provide defense-focused graduate and professional continuing education and research and sustain the technological supremacy of America's air and space forces. AFIT offers masters and doctoral degrees as well as certificates in Information Assurance. Additionally, AFIT offers an Intermediate Developmental Education (IDE) program in Cyber Warfare. The IDE program is a 12 month course of study for mid-grade officers in relevant communities, culminating in a Masters of Science degree.

In March of 2002, AFIT established the Center for Cyberspace Research (CCR) with the stated objective of understanding and developing advanced cyber-related theories and technologies. The CCR is manned predominantly by AFIT faculty from the Department of Electrical and Computer Engineering.

C. Professional Military Institutions (i.e., Service Colleges)

Each service maintains one or more service college(s). These institutions are intended to provide students with in-residence Joint Professional Military Education (JPME). Congressionally mandated JPME qualifications are required to attain the ranks of O-5 and above. For the Navy, attendance at a service college is considered a significant milestone in the professional development of a naval officer and is designed to enhance the competence of those officers with high promotion potential who are selected for attendance. While the service colleges typically award a masters degree upon completion, their primary focus is on strategy and tactics.

D. **Conclusions**

Cyber Warfare and related programs reside within the Computer Science Department at the majority of academic institutions. Based on the committee's review, most institutions desire a classical Computer Science background consisting of the following:

- Programming Skills
    - C, C++, Java
    - Algorithms
    - Data Structures
    - Database (i.e SQL)
    - Operating Systems (desirable but not required)
    - Compiler Design (desirable but not required)
- Networking
    - Protocol to include TCP/IP
    - Computer Architecture
    - Network Architecture
- Math
    - Statistics
    - Linear Algebra
    - Calculus (program dependant)
    - Theory of Computation (desirable but not required)

Currently, USNA's Computer Science curriculum meets these requirements. Additionally, graduate programs are willing to accept students with Math, Physics, Computer Engineering and Electrical Engineering backgrounds. Today's entering information security graduate student is taught the necessary security skills at the graduate level. However, it would seem that a student with information security experience at the undergraduate level would find this prior education to be a major benefit. In the future, information security exposure may become a requirement.

VI. Needs of the CNO and CMC

In an effort to determine what should be accomplished at the undergraduate level, the Committee endeavored to contact OPNAV/CMC staff to determine what knowledge and skills *they* believe general unrestricted line officers—aviators, submariners, surface, USMC ground, etc.—need to possess in order to operate effectively in a cyber warfare environment. Specifically, the Committee attempted to determine what information "Big Navy" expects our graduates to know to contribute in this area when they arrive in the fleet, and what valuable contributions could USNA make? Does the Navy need cyber-capable unrestricted line officers, and, if so, how do we know this?

The need for the military to emphasize cyber warfare skills were mentioned in Chapter 1, in the context of the 2008 CNO Strategic Studies Group, the 2009 White House Cyberspace Policy Review, and the directive mandating the implementation of USCYBERCOM as tasked by the Secretary of Defense. This initiative reinforces the 2007 Cooperative Strategy for 21st Century Seapower [19] and the 2008 National Defense Strategy [20]. As the premier accession source for Navy and Marine Corps Officers, the US Naval Academy has the vision to achieve the dominant role in preparing Junior Officers to fight in the modern battlespace by creating a Cyber Warfare Institute (CWI).

Many operational offices were contacted for proposed guidance in this endeavor. Few substantive results were obtained. Because this initiative is so new, it appears that the Navy has simply not yet formulated any specific guidance for undergraduate education for unrestricted line officers.

The Committee contacted the following commands: Office of the Director of Intelligence Support for the USMC, N7 Office at NNWC, OPNAV N21 Staff, and OPNAV N3/N5 staff. Additional correspondence with Director of IA Division for USMC, BUPERS, and IW CMO yielded little guidance. Coordination between USNA and FLTCYBERCOM for continued URL guidance and training is warranted and should be eased by command proximity after implementation.

The Navy appears to be at the very tip of the iceberg, trying to identify where it is, what it has, and what is needed from both a manpower and developmental perspective. Further information is required. This suggests that a permanent cyber warfare review committee be established for the purpose of cross-discipline curriculum development to further midshipmen exposure in this new warfare environment. This should not preclude the initiative from taking hold immediately in at least a minimal form through professional training and pre-existing academic courses.

VII. Collaborations with Mid-Atlantic Organizations

The Committee explored how our proximity and relationships with mid-Atlantic organizations (e.g., NSA, other Fort Meade commands, the new USCYBERCOM, etc.) might be leveraged through such opportunities as faculty lend/lease, sharing facilities, research opportunities, etc.

A. Potential collaboration sources.

The Committee identified several possible collaborations regarding cyber warfare education, which may be realized due to the geographical proximity of USNA to beltway organizations. While NSA's proximity to USNA suggests that collaboration opportunities would abound, the Committee notes that Fort Meade is a huge base, with approximately 39,000 members and around 35 tenant commands. Moreover, NSA itself, while interested in principle in collaborating with USNA, must see opportunities to further its own goals in order for any collaboration to proceed.

The Committee identified the following organizations as ones with which collaboration on cyber warfare education might be feasible. Also included are the steps the Committee has taken to contact each organization:

- Navy Information Operations Command (NIOC)-Maryland (formerly known as Naval Security Group Activity Fort Meade). NIOC-Maryland is probably the best point of entry for USNA because it is a Navy command and because it will feature significantly in future cyber warfare-related community growth. The Committee contacted LCDR Brian Stites, USN, who is a department head at NIOC-Maryland, as well as an Information Warfare community representative at USNA. The Committee recommends continuing to work outreach issues through LCDR Stites. His contact information is: 40 Department Head, NIOC-MD, Tailored Military Planning Office, 443-479-4235, bmstite@nsa.gov.

- National Security Agency (NSA). USNA currently has a visiting professor from NSA, Dr. Eric Harder, who serves on this Committee and who has access to NSA's research laboratory (NIARL). Through his contacts there he has learned that NIARL is open to ideas that develop with respect to future collaboration but he adds that we must be proactive in order to leverage any interactions.

- Fleet Cyber Warfare Command (FLTCYBERCOM). Based on tasking from OSD, CNO directed N2 to lead a team establishing FLTCYBERCOM with initial operational capability on 01 Oct 09 and full operational capability no later than 01 Oct 10. As the Navy component of USCYBERCOM, FLTCYBERCOM looks to be USNA’s best option for long-term collaboration. As the future focal point for “networks, intelligence, cryptology, information operations, cyber, electronic warfare and space in support of forces afloat and ashore,” FLTCYBERCOM should have an interest in the development of cyber warfare skills and awareness among future Naval and Marine Corps Officers. The Committee recommends maintaining a liaison with NIOC-Maryland personnel, who are involved in the current reorganization efforts. Throughout the period during which this committee met, we were unsuccessful in contacting future FLTCYBERCOM personnel. As their stand-up proceeds, we expect to be able to establish better contacts.

B. Impacts.

The Committee determined that collaboration by midshipmen with NSA already occurs via various internships, though on a very small scale that only includes a handful of midshipmen every year. Educational opportunities on a larger scale would require resolution of numerous logistical issues, most significantly those related to security classifications. While it is possible for midshipmen to receive clearances suitable to maximize educational opportunities at NSA and other tenant commands, the knowledge and experiences they would gain could not easily be expounded upon once they returned to USNA. In short, educational experiences obtained at a classified level must remain at that level. Since USNA undergraduate work exists at an unclassified level, it is currently not feasible to implement a large-scale program given classification realities. In order to work around this obstacle, we would need to identify or help establish programs that focused on educational themes in cyber warfare distinct from operational information and, thus, available at an unclassified level.

The Committee briefly discussed faculty exchange opportunities with Mid-Atlantic organizations. While the Committee was unable to achieve a clear understanding of all aspects of such exchanges, it is clear that these exchanges would offer significantly fewer benefits than those that the midshipmen might realize. With the exception of NIARL, the lion’s share of organizations at which the Committee looked are in the business of providing operational support to deployed forces. As such, faculty would likely be mitigated to roles in these organizations that would not allow them the chance to be truly effective. One area that the Committee suggests for further investigation is in private industry. Perhaps, local corporations focused on cyber defense might be more willing to consider exchange programs with faculty.

A final potential impact of a cyber warfare education initiative deals with facilities. According to the Committee's NAVFAC representative, if USNA partners with NSA/Fort Meade in creating a new shared space for the academic program and satellite operational activities for NSA/Fort Meade, the MILCON project would have a better chance of receiving a higher funding priority. A key aspect of such a project might include the construction of a Sensitive Compartmented Information Facility (SCIF), which would allow midshipmen to work on classified projects as part of their cyber education. While the Committee is cognizant of the multiple obstacles associated with the construction and maintenance of a SCIF—and while the Committee makes no recommendation on building such a facility—such a facility reportedly exists at the U.S. Coast Guard Academy.

C. Benefits.

The Committee believes USNA should further explore the possibility of midshipmen collaborating with cyber warfare organizations, specifically with NIOC-Maryland and the new FLTCYBERCOM. Current midshipmen exposure to such organizations consists of a handful of internships each year, along with orientation visits by about ten midshipmen who have been selected for service assignment in either the Intelligence or Information Warfare communities. The Committee anticipates that if USNA continues to engage NIOC-Maryland as it transitions into the new FLTCYBERCOM structure, then USNA will be well positioned to make the case that it is in these organizations' interest to participate in the education of future officers in the field of cyber warfare.

VIII. Committee Recommendations

In response to the Committee's tasking of examining "how USNA can best ensure that the officers we provide are able to operate effectively in a cyber warfare environment," the Committee offers the following recommendations:

- **Recommendation 1**: Create a required computer science technical core course that addresses the technical foundations of Cyber Warfare.
- **Recommendation 2**: Attain institutional designation as a NSA/DHS National Center of Excellence in IA Education.
- **Recommendation 3**: Create an "Interdisciplinary Cyber Warfare Center" that will serve to enhance midshipmen education in cyber warfare.
- **Recommendation 4**: Create cyber-related electives from interested departments that build upon the core course, and infuse cyber-related topics into existing courses.
- **Recommendation 5**: Add cyber warfare to plebe pro-knowledge.

Each of these recommendations is discussed in detail in the following sections, and is followed by a section discussing the required resources.

Recommendation 1: Create a required computer science technical core course that addresses the technical foundations of Cyber Warfare.

"Cyber Warfare" is a somewhat unusual topic in that it involves a technical academic *core* of tightly inter-related subject matter, as well as a wide range of important topics that, while dependent on the technical core for fullest appreciation, are not dependent on each other. Stated another way, cyber warfare is comprised of, first, a foundational component, dealing with a set of interconnected fundamental technical concepts, and, second, a wide range of interdisciplinary topics, touching upon the areas of law, political science, strategy and tactics, policy, ethics, and the study of foreign languages and culture.

Taking the union of all the subjects in our working definitions of cyber warfare from Chapter I, we have a first draft of the list of topics:

Technical academic core of inter-related subject matter

- **Computer Network[1] Attack (CNA):** Actions taken to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves.
- **Computer Network Defense (CND):** Actions taken to protect, monitor, analyze, detect and respond to unauthorized activity within DoD information systems.
- **Computer Network Exploitation (CNE):** Enabling operations and intelligence collection capabilities to gather data from target or adversary automated information systems or networks.
- **Electronic Warfare** (e.g., jamming, anti-jamming, signal intelligence)
- **Information Assurance**
  - Integrity and Non-repudiation
  - Confidentiality
  - Assured Information Sharing (Authentication)
  - Highly Available Enterprise

Independent stand-alone topics dependent upon the core

- **Psychological Operations**
- **Military Deception**
- **Operations Security**
- **Military Activities** conducted to operate and defend networks
- **Policy** (employment of cyber capabilities where the primary purpose is to achieve military objectives or effects in or through cyberspace).

The Committee recommends that the material designated as the “Technical academic core of inter-related subject matter” be presented in a required computer science technical core course to all midshipmen containing learning objectives similar to those found in Appendix D. The material designated as “Independent stand-alone topics dependent upon the core” are assorted additional topics which allow the student—after gaining mastery of the technical core—to better analyze cyber related decisions as they apply to national and military strategy from social, ethical, legal, ethical and policy viewpoints.

Before presenting a justification for this recommendation, we note that a full understanding and appreciation of the topics listed above under the heading “Technical academic core of inter-related subject matter,” would require the prior presentation of

[1] The reader will note that the word “network” appears frequently in what follows. In an effort to conform with DoD regulations, we borrow several generally accepted terms and acronyms. It must be remembered, though, that a “network” also includes the hosts, applications and protocols that lie at the endpoints, not merely the interconnections between them.

certain prerequisite foundational computing topics, such as *programming, operating systems*, *computer organization* and *networking basics*. While these preliminary concepts are not inherently "cyber," they are essential for understanding cyber; indeed, students can not truly learn about defending computers and networks without prior exposure to this technical foundation. Thus, the Committee's recommendation to create a required computer science technical core course that addresses the technical foundations of Cyber Warfare implies that such a course would also, necessarily, include foundational computing topics.

Justification for this recommendation (five reasons)

1. **The areas listed above as falling under the heading "Technical academic core of inter-related subject matter," are, indeed an interwoven related set of subjects and need to be addressed in a single core course. A core course in cyber warfare, covering the technical academic core, is necessary to lay the cohesive technical foundation required for the midshipmen to be able to comprehend cyber topics when they encounter them in upper level courses, in their Professional Development activities and in the fleet.**

   As an interconnected set of subjects, this material would be best treated in an integrated, coherent, unified presentation. Scattering these topics across the curriculum will lead to a deficient understanding since the causal, logical and contextual relationships between the topics will be necessarily blurred.

   Consider, for example, calculus. A case (indeed, a poor case) could be made that the various topics encountered in calculus might be taught as they arise in other courses. Perhaps, for example, differentiation could be covered when the students first encounter kinematics, and basic integration could be covered when students encounter dynamics, and simple differential equations could be covered when students first encounter electrical circuit analysis. Such a fractured treatment of calculus would cause the students to miss the larger framework.

2. **The U.S. Naval Academy should be on a par with its fellow military academies in treating cyber warfare as a critical academic offering.**

   The U.S. Air Force Academy has integrated the technical academic core areas listed above into a *core course required of all cadets in their freshman year.* The USAFA deems cyber warfare topics important enough to cover them in a core course given to all freshman. The learning objectives for this course are given in Appendix C.

The U.S. Military Academy has, in a similar vein, integrated the technical academic core areas listed above into a *core course required of all cadets who are in Groups II and III*. (At USMA, the Computer Science Department is joined with the Electrical Engineering Department, in what we would call our Division I). The learning objectives for this course are given in Appendix C.

Note that these topics are covered in a course taken by all cadets at USMA, with the exception of those cadets majoring in Civil, Mechanical and Systems Engineering. While it would be unwise to blindly copy what the other service academies are doing, *just because they are doing it*, it would seem prudent to recognize that the other academies believe this subject matter to be critically important.

As an aside, USMA also has a core course, IT105, taken by *all cadets in their freshman year* covering the basics of Information Technology and Computer Science and which is a prerequisite for the upper level IT305.   This course covers, among other topics, fundamentals of computer networks and basic programming.

3. **Midshipmen exposed to a core course in the technical aspects of cyber warfare would be, just from this single course, almost two thirds of the way toward meeting a nationally recognized training standard for information systems security professionals.**

The National Security Agency and the Department of Homeland Security jointly sponsor the National Centers of Academic Excellence in IA Education program. The goal of this program is to reduce vulnerability in our national information infrastructure by promoting higher education and research in IA and producing a growing number of professionals with IA expertise in various disciplines. Each college or university that applies for this designation must pass a rigorous review, demonstrating a commitment to academic excellence in IA education. During the application process, applicants are evaluated against stringent criteria.

To attain designation as a National Center of Academic Excellence in IA Education, an institution must certify that its coursework meets the Committee on

National Security Systems (CNSS) Training Standard 4011. CNSS Training Standard 4011 is titled “National Training Standard for Information Systems Security Professionals,” and provides “the minimum course content for the training of information systems security professionals in the disciplines of telecommunications security and automated information systems security.

At least 60% of the necessary course content delineated in CNSS Training Standard 4011 falls under the topics we have categorized as “Technical academic core of inter-related subject matter” in our description of the subjects comprising cyber warfare. Stated another way, midshipmen exposed to the topics we have categorized as “Technical academic core of inter-related subject matter” would, just from this single course, be almost two thirds of the way toward meeting this nationally recognized training standard for information systems security professionals. Note that the aim here is not to make every naval officer a cyber *specialist*; rather, the aim is to recognize and properly respond to the need to improve cyber *awareness* in every member of the Navy and Marine Corps.

4. **A core course in cyber warfare should be required for all midshipmen due to the heightened emphasis on this issue in recent military policy and strategy.**

More than nuclear power and aviation, cyber is broader, even dualistic in nature, consisting of both a special academic technical component on the one hand, and a set of interdisciplinary topics and tools of political-military action on the other hand. A case can certainly be made that the academic technical component can be offered to a small subset of midshipmen (e.g., Information Technology majors, Computer Science majors and some Electrical Engineering and Computer Engineering majors) whereas the interdisciplinary topics can be offered across multiple disciplines to the Brigade as a whole through incorporation of selected topics within core courses (e.g., a topic in the core military history course (HH104) could discuss the history and development of cyber warfare, and a topic in the core political science course (FP130) might address cyber in the context of government and national security, and the many implications for privacy.

An argument against this approach is that this is, to a large extent, the current practice at USNA, requiring little if any change to what we are already doing. But is this the right approach? Is the Naval Academy curriculum of five years ago still the ideal way to approach the changing environment given the following?

- The CNO notes that "The security challenges confronting Navy information and information systems are multiplying rapidly.... The threats are becoming more sophisticated and diverse, and Navy systems are inherently more vulnerable to surreptitious access, user misuse, abuse and malicious attacks."

- The Pentagon sees fit to establish a new command that will oversee efforts to defend and protect the military's computers and computer networks, and develop offensive cyber-weapons

- The 2008 CNO's Strategic Studies Group recommends as one of three "overarching actions" that the Navy establish an Unrestricted Line Cyber Warfare Community, and, more generally, recommends that the Navy enhance cyber warrior education and training and develop strategies to improve cyber awareness and the ability of every member of the Navy to be cyber-enabled.

- The CJCS National Military Strategy for Cyberspace Operations notes that "DoD personnel operating in cyberspace must have a thorough understanding of the rapidly evolving procedural and technical mechanisms required to conduct cyberspace operations."

- The Chairman of the Joint Chiefs of Staff, Admiral Michael Mullen, expresses his intent to "accelerate and resource our cyberspace efforts—more skilled network operators, a robust global network infrastructure, and a force capable of continued operations while defending against cyber-attacks."

- VADM Dorsett says of the CNO that "his concept is for information management, intelligence, cyber, etc., to form the very foundation of our future Navy."

With all of these events happening in the past two years, can we truly say that the curriculum requires little if any change to what we are already doing?

Furthermore, if cyber-related topics are scattered across the curriculum, various course coordinators across the Yard would, in many cases, be tempted to view their assigned topics as throw-aways, foisted upon them to meet a perceived temporary initiative.

5. **A course in cyber warfare should be taught to all midshipmen due to the pervasiveness of cyber-related issues and tools, and the need for all war fighters to be able to operate in the cyber domain.**

A case can certainly be made that there should not be a mandatory core course dedicated to cyber warfare because there are, after all, no dedicated core courses directed to Air Warfare, Surface Warfare, Undersea Warfare, etc. If we are to treat Cyber Warfare as a new operating environment, what would be the purpose of holding a mandatory course in this environment and not others?

An answer to this question would proceed along several lines. First, there ***are*** dedicated core courses that provide a foundation for air, surface and undersea warfare. Courses in *Naval Weapons Systems*, *Fundamentals of Seamanship*, *Introduction to Navigation*, *Navigation and Piloting*, and two *Electrical Engineering* courses exist in the present core precisely to provide the technical foundation for officers in these warfare disciplines. Midshipmen are not trained specifically to operate in the air or under the sea. Instead, they are trained in the basics of hard science to be applied in specific warfare fields. Likewise, a foundation must be provided for officers to operate in the cyber domain. As more military officers find themselves engaged in fighting in cyberspace, they will increasingly need a thorough understanding of the basic technical concepts that underlie battle in this domain. There exists a core of technical academic material that can prepare officers to understand and operate in this domain.

Second, the notion that there is an academic core involved in training for cyber warfare (as opposed to a training core that might be found at aviation training, or submarine school) is reinforced by the fact that IP officers are sent to NPS for an academic master’s degree.

Third, this notion of a strong academic requirement is reflected also in the recruitment of the civilian cyber workforce as well. For example, the DoD has a Department of Defense Information Assurance (IA) Scholarship Program (IASP) designed to increase the number of new entrants to DoD who possess key Information Assurance and IT skill sets and to serve as a tool to develop and retain well-educated military and DoD civilian personnel who support the Department’s critical IT management and infrastructure protection functions. Relevant academic disciplines for the scholarship program include Mathematics, Biometrics, Electrical Engineering, Electronic Engineering, Computer Science, Computer Engineering, Software Engineering, Computer Programming, Computer Support, Data Base Administration, Computer Systems Analysis, Operations Research, Information Security (Assurance), and Business Management or Administration. Although the list of academic disciplines is not limited to this list, any academic discipline chosen ***must*** include a concentration in Information Assurance.

Recommendation 2: Attain institutional designation as an NSA/DHS National Center of Excellence in IA Education.

The National Security Agency and the Department of Homeland Security cosponsor the National Centers of Excellence in Information Assurance Education program to promote education in information assurance.

To receive this designation, an institution must certify that it meets stringent criteria in regards to its curriculum, faculty and research, and, additionally, must demonstrate an institution-wide commitment to information assurance practices and education. The program is only open to regionally accredited 4-year colleges and universities (i.e., not community colleges).

Approximately 2% of the colleges and universities in the United States have garnered the distinction of becoming a National Center of excellence in Information Assurance Education. The USMA and USAFA have long ago garnered this distinction, and have greatly benefited from the funding sources made specifically available to institutions that hold NSA/DHS National Center of Excellence in IA Education designations.

Justification for this recommendation

Designation as a National Center of Excellence in Information Assurance Education confers several benefits to USNA:

- By obtaining this designation, an institution is eligible to apply for "capacity building" grants from the National Science Foundation and the National Security Agency to expand their program in information assurance. These grants can be used to improve infrastructure, provide training and fund initiatives not otherwise affordable.

- By obtaining this designation, an institution can partner with other National Centers of Excellence in Information Assurance Education on information assurance-related grants.

- Several private companies (Cisco, for example) are willing to donate state-of-the-art equipment to institutions that obtain designation as a National Center of Excellence in Information Assurance Education.

- By obtaining this designation, an institution is assigned a Senior Executive Academic Liaison to act as the institution's advocate within NSA. This liaison serves as a point-of-contact for grants, funding requests and related issues.

- By obtaining this designation, an institution can provide internships to civilian graduate students, with the internship salaries paid for by the graduate student program administrators (e.g., DHS, NSF, OPM), not USNA.

Note that the National Center of Excellence in Information Assurance Education designation would be an *Academy* credential, not the credential of any individual department. It is also worth noting that civilian institutions *must* be designated as a National Center of Excellence in Information Assurance before applying for NSA and NSF information assurance-related grants.

Recommendation 3: Create an "Interdisciplinary Cyber Warfare Center" that will serve to enhance midshipmen education in cyber warfare.

The Center will:

- Serve as a focal point for cyber education, assisting in cyber warfare curriculum development and instruction across the Yard, and endeavoring to infuse cyber topics across the curriculum.

- Encourage, facilitate and conduct research with students and faculty (both in-house and with outside agencies).

- Coordinate with the USNA Research Office to and facilitate cyber-related internships with NSA, NRL, DISA, Naval Warfare Development Command

- Oversee an interdisciplinary Midshipman Cyber Warfare Club that will increase cyber awareness across the ***entire*** student body (not just CS/IT/EEE/ECE) through a host of innovative activities such as
  - Practice hands-on network defense and attack operations
  - Run cyber defense/attack competitions and games
  - Invite distinguished guest lecturers for presentations open to all students and faculty

The Committee recommends anchoring the various cyber warfare-related efforts in a Center, where the word "*Center*" is used in a general sense, the point simply being that some formal organization should exist where faculty and students can share their research, collaborate and interact with each other.

Justification for this recommendation

1. **The Center will provide the necessary support and coordination to ensure the integration of cyber awareness into midshipmen education.**

   The existence of this formal organization will indicate the Academy's seriousness of purpose, will indicate clear institutional support, and will serve to raise the visibility of cyber warfare-related efforts across the Yard. The Committee believes that a collection of dispersed efforts— not rooted in a Center—will not be sufficient.

   By providing a focal point for the sharing of expertise and perspectives across the Yard, this Center will help coordinate and integrate efforts to infuse cyber awareness into the education of midshipmen. The Center would provide a streamlined means of identifying priorities, collecting and disseminating information, harmonizing efforts and shaping a common framework for action. Without such a Center, a complex patchwork of overlapping initiatives might result, leading to an unclear delineation of goals, uneven and inconsistent results and duplication of effort.

2. **An institution must have a designated center in order to be designated as a National Center of Excellence in Information Assurance Education (see Recommendation 2, above).**

   As mentioned in Chapter IV, the other service academies have such Centers: USAFA has the *Academy Center for Cyberspace Research* and USMA has the *Information Technology and Operations Center*.

Recommendation 4: Create cyber-related electives from interested departments that build upon the core course, and infuse cyber-related topics into existing courses.

As mentioned, cyber warfare has a technical side, but it also encompasses a variety of non-technical unconnected interdisciplinary topics falling under the general headings of:

- **Psychological Operations**
- **Military Deception**
- **Operations Security**
- **Military Activities** conducted to operate and defend networks
- **Policy** (employment of cyber capabilities where the primary purpose is to achieve military objectives or effects in or through cyberspace).

Justification for this recommendation

Multiple courses covering the previously listed topics are critically important for a full understanding of cyber warfare—the *whole* cyber warrior, as it were.

This recommendation requires less justification because this recommended action has already started to occur, albeit in fits and starts. As described in Appendix A, cyber warfare has recently appeared in courses offered by the Political Science Department (*Politics of Irregular Warfare*, *National Security Policy* and *Future Global Security Challenges* electives) and the History Department (*Rise of the Machines*, *Technological Change in War and Peace* and *The Information Age: From the ENIAC to the X-Box* electives) and the Physics Department (*Quantum Information* elective).

The Committee feels that it is very important that faculty in Division III not be told: "Teach cyber warfare." Rather, the approach should be (through the aforementioned Center) to develop a mindset that would inculcate the idea that cyber warfare covers many aspects of a warrior's education and training; not just grounding in the technical fundamentals. A Center could assist in showing how cyber related topics could be weaved into the academic program, with all final curricula decisions left to the individual Departments. One could easily imagine courses in such topics as those above, as well as *Cyber Law* and *History of Terrorism* being of interest to students and faculty alike.

Recommendation 5: Add cyber warfare to plebe pro-knowledge.

Midshipmen should receive professional training in cyber warfare, in addition to the recommended academic instruction.

The Center should work with the Professional Programs Department and Officer Development Department to incorporate cyber warfare information into the plebe "pro-book." Those portions of the developing the cyber warrior that fall under the category of "training" can and should be conducted in Bancroft Hall. Such topics can also be developed into training modules that can be distributed throughout the entire Brigade of Midshipmen. Adding cyber warfare topics to the plebe pro-knowledge book would inculcate in the midshipmen the importance of this area from the start of their experience at USNA.

IX. Required Resources.

In an effort to provide structure for how USNA might go about implementing the Committee's recommendations, the following three categories are defined:

Foundational. These recommendations provide the minimal cyber-related modifications to the USNA curriculum, facilities, and activities that should be done for

- the entire Brigade of Midshipmen, as well as modifications for
- a major portion of the Brigade, as well as modifications for
- just a small subset of the Brigade.

The Committee feels that the Foundational modifications are those that are necessary to produce cyber-capable unrestricted line officers that meet the needs of the Navy ***at some foundational level***.

Proficient. These recommendations provide the cyber-related modifications to the USNA curriculum, facilities, and activities that should be done for

- the entire Brigade of Midshipmen, as well as modifications for
- a major portion of the Brigade, as well as modifications for
- just a small subset of the Brigade.

The Committee feels that the Proficient modifications are those that are necessary to produce cyber-capable unrestricted line officers that meet the needs of the Navy ***at an enhanced level*** in the information-intensive skills that the Director of Naval Intelligence expects to form the foundation of the future Navy.

Dominant. These recommendations provide the cyber-related modifications to the USNA curriculum, facilities, and activities that should be done for

- the entire Brigade of Midshipmen, as well as modifications for
- a major portion of the Brigade, as well as modifications for
- just a small subset of the Brigade.

The Committee feels that the Dominant modifications are those that are necessary to produce cyber-capable unrestricted line officers and that would position USNA to support the CNO's vision of playing ***a dominant role*** in the information-intensive skills that the Director of Naval Intelligence expects to form the foundation of the future Navy.

Table 2 below shows the Committee's recommendations as organized by a desired level of cyber education. Table 2 is intended to be used as follows: A row should be selected to indicate the level of cyber education desired. The columns within the selected row give the actions that should be taken for All, Many, and a Few of the midshipmen in order to attain that row's level of cyber education.

Table 2. Recommendations Organized by Desired Level of Cyber Education.

	All	Many	Few
Foundational	• computer science technical core course • Add cyber warfare to plebe pro-knowledge • Attain Institutional NSA/DHS CAE-IA certification	• cyber-related electives from interested departments that build on the computer science technical core course. • Cyber warfare club	• Cyber Defense Exercise (CDX) for a few • Cyber-related internships • Establish Cyber Warfare Center for a few
Proficient	• computer science technical core course • Add cyber warfare to plebe pro-knowledge • Attain Institutional NSA/DHS CAE-IA certification • cyber topics integrated into PRODEV courses	• Interdisciplinary cyber tracks • Cyber-related internships • Establish Cyber Warfare Center for many	• CDX for a few • Cyber exposure in some warfare practicums • Cyber-related summer training • CDX-like interdisciplinary events for a few more (broader reach) • Cyber Scholars (like Bowman Scholars, but driven by IP/IW/Intel vice submarines)
Dominance	• computer science technical core course • Add cyber warfare to plebe pro-knowledge • Attain Institutional NSA/DHS CAE-IA certification • cyber topics integrated into PRODEV courses • Professional Core Competencies (PCCs) modified to address cyber warfare	• Interdisciplinary cyber tracks. • Cyber-related internships • Establish Cyber Warfare Center for many • CDX-like events for many mids • cyber warfare summer training	• CDX for a few • Cyber Scholars • Multi-Disciplinary Cyber Warfare Major similar to Quantitative Economics

Required Resources at Each Level (based on desired level of cyber education):

Foundational. Required resources: 10 FTEs and 4 general purpose classrooms for the computer science technical core course.

- Assuming that the computer science technical core course can be taught (as it is at USAFA) as a 3-0-3 course to half of a class each semester using general classrooms with electrical power and wireless connections and issued laptops, 10 FTEs and 4 dedicated classrooms (i.e., the dedicated assignment of 4 *existing* classrooms) are required.
- Curriculum development proposals will likely be required.
- The Cyber Warfare Club could be run as an ECA requiring an officer rep and a faculty rep.
- The director of Cyber Warfare Center could be a collateral duty for a faculty member from the computer science department and would focus mainly on maintaining the Institutional NSA/DHS CAE-IA certification.
- The remainder actions shown in the Foundational row are already being done at USNA.

Proficient. Required resources: 10 FTEs and 4 general purpose classrooms for the computer science technical core course, plus a billet and office space and staffing for a director of the Cyber Warfare Center.

- Assuming that the computer science technical core course can be taught (as it is at USAFA) as a 3-0-3 course to half of a class each semester using general classrooms with electrical power and wireless connections and issued laptops, 10 FTEs and 4 dedicated classrooms (i.e., the dedicated assignment of 4 *existing* classrooms) are required.
- Curriculum development proposals will be required.
- The Cyber Warfare Club could be run as an ECA requiring an officer rep and a faculty rep.
- The director of the Cyber Warfare Center could be a primary duty for a PMP faculty member or organized as an endowed chair. This director would:
    - Maintaining the Institutional NSA/DHS CAE-IA certification,
    - Foster relationships in the IP/IW/Intel communities to enable ‘Cyber Scholars’ which could be organized much like Bowman Scholars.
    - Assist departments desiring to enhance the cyber warfare aspects of some of the courses or establish new electives.

Dominant. Required resources: 10 FTEs and 4 general purpose classrooms for the computer science technical core course, plus a billet and office space and staffing for a director of the Cyber Warfare Center, plus 3 additional FTEs, 2 additional general purpose classrooms, and 2 sandboxed networking labs and equipment with support staff for CDX-Like events for up to 120 midshipmen per semester.

- Assuming that the computer science technical core course can be taught (as it is at USAFA) as a 3-0-3 course to half of a class each semester using general classrooms with electrical power and wireless connections and issued laptops, 10 FTEs and 4 dedicated classrooms (i.e., the dedicated assignment of 4 *existing* classrooms) are required.
- Curriculum development proposals will be required.
- The Cyber Warfare Club could be run as an ECA requiring an officer rep and a faculty rep.
- The director of the Cyber Warfare Center could be a primary duty for a PMP faculty member or organized as an endowed chair. This director would:
    - Maintain the Institutional NSA/DHS CAE-IA certification,
    - Foster relationships in the IP/IW/Intel communities to enable 'Cyber Scholars' which could be organized much like Bowman Scholars.
    - Assist departments desiring to enhance the cyber warfare aspects of some of the courses or establish new electives
    - Support the development of cyber-related summer training.
- The establishment of a non-accredited, interdisciplinary Cyber Warfare major similar in structure to Quantitative Economics could be considered.
- Two sandboxed (unreachable from the Internet) networking labs and a technical support staff with computer equipment to allow up to 120 midshipmen to participate in a CDX-like event per semester.

The Committee recommends establishing cyber-related modifications to the USNA curriculum, facilities, and activities at the Foundational level. We summarize the resources needed for the Foundational level in Table 3 below.

Table 3. Resources Required at Each Level of Cyber Education.

	Requirement	**Justification**
Foundational	• 10 faculty FTEs • 4 dedicated general purpose classrooms with wireless connectivity plus • 1 lab tech support.	• 600 students taking a 3-0-3 course each semester, with a section size of 20, would entail 30 sections. An FTE could therefore teach three sections, so 10 FTEs needed. • 30 sections, each 3-0-3, requiring 90 hours of instruction. One classroom can be scheduled for 30 hours in an academic week. If perfect scheduling could be arranged, 3 classrooms would suffice. To avoid scheduling conflicts, 4 classrooms are recommended. 1 Tech support personnel required for the labs.
Proficient	• 10 faculty FTEs • 4 dedicated general purpose classrooms with wireless connectivity plus tech support. • 1 lab tech support.	• The 600 students taking a 3-0-3 course as described above with FTEs and classroom requirements as described in the row above. • A FTE billet plus office space and staffing for a dedicated, full-time, director of the Cyber Warfare Center whose role it would be to oversee the center and pursue funding opportunities.
Dominant	• 13 faculty FTEs • 6 dedicated general purpose classrooms with wireless connectivity plus tech support. • 2 sandboxed networking labs. • 2 lab tech support.	• In addition to the 600 students taking a 3-0-3 course as described above, an additional 120 students per semester take advanced technical cyber course work and participate in CDX-like structured events. • A FTE billet plus office space and staffing for a dedicated, full-time, director of the Cyber Warfare Center as described in the row above.

X. Conclusions

The Committee recommends certain modifications to the USNA curriculum, facilities, and activities deemed necessary to produce cyber-capable unrestricted line officers that meet the needs of the Navy ***at some foundational level***.

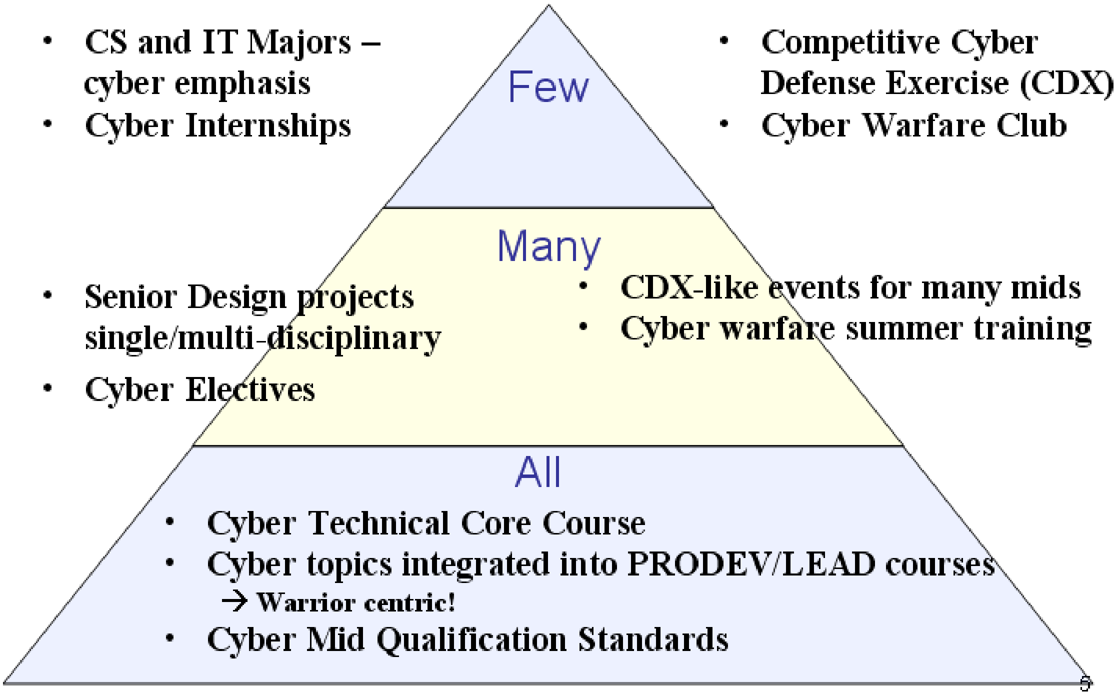
Specifically, in its Aug 12th meeting the Committee unanimously agreed on the following five recommendations (with a summary of the recommendations given in Figure 1):

- **Recommendation 1:** Create a required computer science technical core course that addresses the technical foundations of cyber warfare. A core course in cyber warfare, covering the technical academic core of the subject, would lay the cohesive technical foundation required for midshipmen to be able to comprehend cyber topics when they encounter them in upper level courses, professional development and in their careers in the fleet. Such a course would also place the U.S. Naval Academy on a par with its fellow military academies in treating cyber warfare as a critical academic offering.
- **Recommendation 2**: Attain institutional designation as a NSA/DHS National Center of Excellence in IA Education.
- **Recommendation 3**: Create an "Interdisciplinary Cyber Warfare Center" that will serve to enhance midshipmen education in cyber warfare. The Center would provide the necessary support and coordination to ensure the integration of cyber awareness into midshipmen education throughout the Yard.
- **Recommendation 4**: Create cyber-related electives from interested departments that build upon the core course, and infuse cyber-related topics into existing courses. A variety of courses covering the independent interdisciplinary aspects of cyber warfare would aid in providing a full understanding of cyber warfare—the *whole* cyber warrior, as it were.
- **Recommendation 5**: Add cyber warfare to plebe pro-knowledge. Midshipmen should receive professional training in cyber warfare, in addition to the recommended academic instruction.

Although several options exist for implementing the Committee's recommendations, an alternative might begin with running just a few sections of the proposed required computer science core course that addresses the technical foundations of cyber warfare. Such a course has already been developed by the Computer Science Department and is being considered as a course offering for Spring AY10. After evaluating the results of this offering, a prototype course could be considered for additional groups of midshipmen such as General Science and General Engineering Majors. Once these larger offerings have been evaluated and the required faculty brought on board, the course could then be offered to all midshipmen in a given class year.

The Committee feels that implementing these recommendations is necessary in order to produce cyber-capable unrestricted line officers that meet the needs of the Navy at what we define as a 'Foundational Level'. Higher levels of engagement (Proficient and Dominant) have also been considered as discussed above, and may be considered after the Foundational Level has been met. It is estimated that attaining the Foundational Level recommendations would require the hiring of 10 FTEs (full-time equivalent) faculty members, and the dedicated use of four standard classrooms that already exist in Michelson Hall but are currently being used for Language Studies.

Figure 1: Summary of Cyber Warfare Committee Recommendations for USNA to contribute to the CNO's vision of Cyber Dominance.


• CS and IT Majors – cyber emphasis
• Cyber Internships
Few
• Competitive Cyber Defense Exercise (CDX)
• Cyber Warfare Club
Many
• Senior Design projects single/multi-disciplinary
• Cyber Electives
• CDX-like events for many mids
• Cyber warfare summer training
All
• Cyber Technical Core Course
• Cyber topics integrated into PRODEV/LEAD courses
→ Warrior centric!
• Cyber Mid Qualification Standards
5

Appendix A: Cyber Warfare Related Courses that are Currently or have Been Previously Taught at USNA

Division of Engineering and Weapons

Course Number/Title: EE302 Electronic Communication Systems and Digital Communications

Description: There are a few topics that are briefly discussed that deal with frequency hopping, spread spectrum, and encryption.

Semesters taught: Fall and Spring

Students enrolled: ~650

Infrastructure requirements: None

Audience: All Division 2 and 3

Course Number/Title: EE332 Electrical Engineering II

Description: There are a few topics that are briefly discussed that deal with frequency hopping, spread spectrum, and encryption.

Semesters taught: Spring

Students enrolled: ~100

Infrastructure requirements: None

Audience: Systems (ESE) students

Course Number/Title: EE334 Electrical Engineering and IT Systems

Description: There are a few topics that are briefly discussed that deal with frequency hopping, spread spectrum, and encryption.

Semesters taught: Spring

Students enrolled: ~200

Infrastructure requirements: None

Audience: Division 1 (non ECE and EEE and ESE)

Course Number/Title: EE354 Modern Communication Systems

Description: There are a few topics that are briefly discussed that deal with coding schemes, encryption, and avoiding intercept.

Semesters taught: Spring

Students enrolled: ~40

Infrastructure requirements: Signal generators, mixers, amplifiers, filters, o-scopes, spectrum analyzers

Audience: ECE and EEE majors

Course Number/Title: EE433 Wireless and Cellular Communications Systems

Description: There are a few topics that are briefly discussed that deal with coding schemes, encryption, and avoiding intercept.

Semesters taught: Fall

Students enrolled: ~20

Infrastructure requirements: Signal generators, mixers, amplifiers, filters, o-scopes, spectrum analyzers

Audience: ECE and EEE Elective

Course Number/Title: EE435 Biometrics

Description: In this course, students will evaluate the performance of state-of-the-art systems for identifying an individual through biometric signals (iris scans, facial parameters, fingerprints, voice prints). Individual design projects will be performed that develop and analyze alternative algorithms for identification, or that combine two systems into a multi-sensor identification system.

Semesters taught: Spring

Students enrolled: ~20

Infrastructure requirements: Computer lab and various software.

Audience: ECE and EEE Elective

Course Number/Title: EE464 Introduction to Computer Networks

Description: There are a few topics that discuss security related tools, including firewalls, private/public keying, encryption, and RSA. There is also a lab that demonstrates the ability to steal information from the internet. In particular, students rip off IM messages that are being sent over the internet.

Semesters taught: Fall

Students enrolled: ~20

Infrastructure requirements: Computer lab with network connectivity and software.

Audience: ECE and EEE Elective

Course Number/Title: ES300 Introduction to Naval Weapons Systems

Description: An introduction to weapons systems applications of RADAR, electro-optics, SONAR, engagement systems, destruction systems and system integration. The discussion on electronic warfare may be relevant to Cyber Warfare.

Semesters taught: Fall, Spring, Summer

Students enrolled: ~500

Infrastructure requirements: None

Audience: Core course

Course Number/Title: EA 463 Space Operations

Description: This course investigates the relationship between mission operations and the other elements of a space mission. It defines a process for translating mission objectives and requirements into a viable mission operation concept. The course focuses on how we get information to and from space and then to the user in a usable format.

Semesters taught: Sporadic

Students enrolled: Varies

Infrastructure requirements: None

Audience: EA Majors (Astro Track only) elective

Periodicity issues: This course is offered sporadically based on student interest and enrollment

Division of Mathematics and Science

Course Number/Title: SP484A Topics in Quantum Mechanics: Quantum Information

Description: Investigation of the bases and science behind quantum key distribution (aka quantum cryptography) and quantum computation, key technologies for the future of cyber security and information assurance.

Semesters taught: Spring 2009,

Students enrolled: 8

Infrastructure requirements: Visit and hands on with Quantum computation laboratory at JHU APL (Dr. Bryan Jacobs)

Audience: Physics major OR special permission after taking Modern Physics

Periodicity issues: Can only run with support from the department to allow instructor with basis in basic quantum mechanics.

Course Number/Title: SI200: Information Technology for the Junior Officer

Description: The focus of this course is practical applications of personal computers for the junior officers in the fleet. Topics include: structured and object oriented computer programming, designing, implementing, and querying databases using a Database Management System, computer architecture and networking basics, information assurance and human-computer interaction.

Semesters taught: Spring

Students enrolled: ~20

Infrastructure requirements: Computer lab

Audience: Required course for General Science (SGS) majors

Course Number/Title: IT285: Cyber Warfare

Description: This course integrates military information operations, intelligence, and networks in the air, sea, land, space and cyberspace domains. Topics include networks, information assurance, defense against hackers, and web development from a cyber warfare perspective.

Periodicity issues: This course is currently under development and will be offered to midshipmen as an elective in Spring 2010. The intent is that this course will be available to *all* midshipmen; no prior knowledge of computer programming or networks would be required.

Course Number/Title: SI250: Information Systems for the Junior Officer

Description: The primary emphasis of the course is practical applications of personal computers and the Internet in the Fleet/Fleet Marine Force (FMF), with coverage of some special tactical computers as well. Application software is addressed from a junior officer's viewpoint, as an operational unit Branch/Division/Company Officer or as a support staff member.

Semesters taught: Occasional offering

Students enrolled: ~5

Infrastructure requirements: Computer lab

Audience: Elective for any interested midshipmen

Periodicity issues: Offered occasionally based on student interest, last offered Sp 2008

Course Number/Title: IT430 Information Assurance and Network Security

Description: This course is an introduction to the theoretical and practical facets of Information Assurance (IA) to include: Policies and directives, Trusted systems, Access mediation, Cryptography, Public Key Infrastructure, Information Warfare, Network security and Database security.

Semesters taught: Spring and Fall (usually)

Students enrolled: 30-40

Infrastructure requirements: Computer lab with online network and sandbox network

Audience: CS/IT Majors (Prereq – IC322 Networks)

Course Number/Title: IT432 – Advanced Information Assurance and Network Security

Description: This course provides an introduction to topics in secure system design, including: cryptography, operating system security, and language based security. Where the IT430 course focuses primarily on securing an existing system, this course studies how to design a system to meet security goals.

Semesters taught: Spring

Students enrolled: 10-20

Infrastructure requirements: Computer lab with online network and sandbox network

Audience: CS/IT Majors (Prereq – IT430 IA and Info Assurance)

Course Number/Title: IC322 – Computer Networks

Description: The course presents the fundamental theoretical concepts, characteristics and principles of computer communications and computer networks, and analyzes and assesses these foundational concepts with respect to network performance and network design.

Semesters taught: Fall

Students enrolled: 35-40

Infrastructure requirements: Computer lab with an online network as well as a sandbox network. Routers and Switches.

Audience: CS/IT Majors (Prereq – IT221 Systems)

Course Number/Title: IT495A – IPV6: Practical Uses in Military Networks

Description: This course focuses on applications of the new internet protocol, including security aspects.

Semesters taught: Fall 2009

Students enrolled: 1 Student (Independent Study)

Infrastructure requirements: Trident Research Lab

Audience: CS/IT Majors

Periodicity issues: This course is no longer available because it was an independent study conducted by one student for one semester.

Course Number/Title: SI485H – Cryptography and Network Security

Description: This course introduces the principles of cryptography with applications to network security.

Semesters taught: Fall 09

Students enrolled: 15

Infrastructure requirements: Computer lab with an online network as well as a sandbox network.

Audience: CS/IT/EE Majors (Prereq – IC322 Networks or EE464 Intro to Computer Networks)

Periodicity issues: This course is offered sporadically based on interest from CS/IT student surveys.

Course Number/Title: IT486A – Wireless Networks

Description: This course focuses on the fundamentals of wireless networks,

Semesters taught: Spring 09

Students enrolled: 7

Infrastructure requirements: Computer lab with wireless network. Handheld PDAs for wardriving.

Audience: All Majors (Prereq – Prior Programming Experience)

Periodicity issues: This course is offered sporadically based on interest from CS/IT student surveys.

Course Number/Title: IT495 – IPV6: Capabilities and Operational Concepts

Description: This research will entail building, operating and maintaining a pilot IPv6 network between USNA and USMA. .

Semesters taught: Fall 08

Students enrolled: 1 (Independent Study)

Infrastructure requirements: Trident Research Lab

Audience: CS/IT Majors

Periodicity issues: This course is no longer available because it was an independent study conducted by one student for one semester.

Course Number/Title: IT350 – Web & Internet Programming

Description: Web site design and management, clients and servers, client and server side scripting languages, web transmission protocols. A basic understanding of web programming fundamentals is crucial to implementing proper security in online projects such as websites.

Semesters taught: Fall

Students enrolled: 30

Infrastructure requirements: Web Drive and Computer Lab

Audience: CS/IT Majors

Course Number/Title: IT452 – Advanced Web & Internet Systems

Description: Web server design and configuration, search engine design and usage, web security and authentication, server implementations, web collaboration mechanisms, web services, and knowledge representation on the web. The sections of the course that focus on web security and authentication are imperative to a proper understanding of cyber warfare.

Semesters taught: Fall

Students enrolled: 10

Infrastructure requirements: Web Drive and Computer Lab

Audience: CS/IT Majors (Prereq - IT350 Web Programming)

Course Number/Title: SM486C Introduction to Cryptography

Description: N/A

Semesters taught: Spring 2009

Students enrolled: 1

Infrastructure requirements: None

Audience: Math Majors

Periodicity issues: Reading Course

Course Number/Title: SM473 Cryptography

Description: Students will read and make presentations on topics determined by the instructor. Each student will complete a project on a topic to be agreed upon by the instructor and student.

Semesters taught: Spring 2008

Students enrolled: 7

Infrastructure requirements: None

Audience: Math Majors

Periodicity issues: Capstone Course

Course Number/Title: SM496 A Small Exponent Attach on RSA

Description: N/A

Semesters taught: Spring 2008

Students enrolled: 1

Infrastructure requirements: None

Audience: Math Majors

Periodicity issues: Math Honors Project

Course Number/Title: SM496 Secure Sockets Layer

Description: Research Project

Semesters taught: Spring 2008

Students enrolled: 1

Infrastructure requirements: None

Audience: Math Majors

Periodicity issues: Research course

Course Number/Title: SM496 Aspects of Elliptic Curve Cryptography and Schoof's Algorithm

Description: Research Project

Semesters taught: Spring 2007

Students enrolled: 1

Infrastructure requirements: None

Audience: Math Majors

Periodicity issues: Research course

Course Number/Title: SM496 Linear Feedback Shift Registers and Cyclic Codes in SAGE

Description: Research Project

Semesters taught: Spring 2006

Students enrolled: 1

Infrastructure requirements: None

Audience: Math Majors

Periodicity issues: Research course

Course Number/Title: SM496 Nearly Involutive Matrices for the Keyspace of the Hill Cipher

Description: Research Project

Semesters taught: Spring 2006

Students enrolled: 1

Infrastructure requirements: None

Audience: Math Majors

Periodicity issues: Research course

Course Number/Title: SM496 Long Quadratic Residue Codes

Description: Research Project

Semesters taught: Spring 2006

Students enrolled: 1

Infrastructure requirements: None

Audience: Math Majors

Periodicity issues: Research course

Course Number/Title: SM496 Low Density Parity Check Codes

Description: Research Project

Semesters taught: Spring 2006

Students enrolled: 1

Infrastructure requirements: None

Audience: Math Majors

Periodicity issues: Research course

Division of Humanities and Social Sciences

Course Number/Title: FP384, Politics of Irregular Warfare

Description: Cyber warfare was discussed for parts of two class periods. 1. As it relates to 4th generation warfare as well as a potential primary tactic in "5th generation warfare." Also, it is discussed a type of terror tactic perpetrated by non-state or sub-state actors. Estonia and Georgia are used as recent examples.

Semesters taught: Continuous

Students enrolled: 50 each semester

Infrastructure requirements: Classroom

Audience: Political Science majors are the majority, but it is open to all majors.

Periodicity issues: Will be down the one section next fall, which is not ideal

Course Number/Title: FP490, Information Technology Capstone

Description: Culminating course taught to Political Science majors during their first class year. Projects dealt with some kind of cyber security issue; some midshipmen formed teams that competed in cyber warfare competitions.

Semesters taught: Fall/Spring, 2006-07

Students enrolled: approx. 25

Infrastructure requirements: Classroom, occasional computer lab access

Audience: senior Political Science majors

Periodicity issues: Course no longer taught following IT major restructuring

---

Course Number/Title: FP313, Information Technology and International Relations

Description: Effects on information technology on both the national and international political systems; emphasis on changed weaponry, the vulnerability of cyberspace and other aspects of the information revolutions on the relations among nations

Semesters taught: Fall/Spring 2004-07

Students enrolled: 20 per sem.

Infrastructure requirements: Classroom

Audience: Open to any midshipmen; prereq: FP210

Periodicity issues: Main instructor no longer teaching here; course not currently offered

---

Course Number/Title: FP407, Intelligence and National Security

Description: Examination of nature, significance and development of intelligence including collection, counterintelligence, clandestine, and covert action and evaluation; includes current issues and case studies. Cyber warfare is discussed in the context of how it is increasingly used by other nations and non-state actors to influence events, as well as how the U.S. Intelligence Community works to defend the nation's computer networks and other infrastructure.

Semesters taught: Continuous

Students enrolled: 50

Infrastructure requirements: Classroom

Audience: 1/c or 2/c midshipmen, prereq: FP130, 210/230

Periodicity issues: Normally taught by the active duty intelligence officer assigned to the Political Science Department; other civilian faculty have taught on occasion

---

Course Number/Title: FP421, National Security Policy

Description: Cyber warfare has figured in more recent semesters during lessons about the Navy's Cooperative Strategy for 21st Century Sea Power, wherein cyberspace is noted as key to the Navy's expanded core capability of Sea Control. Cyber warfare is also discussed in relation to the desire/ability of armed groups to exploit this domain. Finally, cyber warfare is discussed as a counterweight to traditional elements of national power.

Semesters taught: Continuous

Students enrolled: 24-48

Infrastructure requirements: Classroom

Audience: Open to any midshipman who has completed FP130

Course Number/Title: FP460, Future Global Security Challenges

Description: Examines the complex and fluid security environment of the 21st Century and exposes midshipmen to analytic tools to function in that environment. The course looks at cyber-related issues in the context of underlying forces shaping future global and U.S. security. Cyber warfare is specifically examined as an emerging global problem.

Semesters taught: Fall, Spring, 2007-09, four semesters total

Students enrolled: 20 per sem.

Infrastructure requirements: Classroom

Audience: Open to any midshipman; prereq: FP130, FP210

Periodicity issues: Taught by David C. Gompert of the RAND Corporation; course is not currently offered since instructor is no longer in the department.

Course Number/Title: HHXXX, Rise of the Machines: Technological Change in War and Peace

Description: Course provides historical background for emergence of complex technical systems, to include rise of telephone system and automated weapons systems. (Will read Singer's "Wired for War"; and use Boots' book, "War Made New").

Semesters taught: Pending for fall, 2009

Students enrolled: approx. 15 per sem.

Infrastructure requirements: Classroom

Audience: open to any midshipman

Periodicity issues: None, course will debut this fall.

Course Number/Title: HH379, History of IT Revolutions

Description: Provided a background of emergence of computer industry and internet.

Semesters taught: 2001-2005

Students enrolled: 15 per sem.

Infrastructure requirements: Classroom

Audience: Formerly a requirement for IT majors; open to all midshipmen

Periodicity issues: Course no longer offered. The professor (Kurt Beyer) left the Academy, and before a replacement could be hired the course requirement for IT majors was cancelled

---

Course Number/Title: HH104, Naval History

Description: Core military history course, and in the course of naval history does cover the Cold War and the rise of electronic warfare, code-breaking, and computers (e.g., ENIGMA, COLLOSSUS, ENIAC, NTDS, etc.)

Semesters taught: Continuous

Students enrolled: 1200 per year

Infrastructure requirements: Classroom

Audience: Required of all midshipmen

Course Number/Title: HH485, The Information Age: From the ENIAC to the X-Box

Description: Upper-level course that examined technological innovations during the second half of the 20th Century and beyond.

Semesters taught: fall 2004-fall 2005

Students enrolled: 15-20 students per sem.

Infrastructure requirements: Classroom

Audience: Required of all midshipmen

Periodicity issues: Course no longer offered. The professor (Kurt Beyer) left the Academy

---

Division of Professional Development/Officer Development

Course Number/Title: NS410 Network Centric Warfare

Description: NS410 focused on the application of information technology in warfare and emerging asymmetric threats. The course did not have a major focus on cyber warfare, but retained a holistic view of Command and Control policies and the importance of information technology in war. The curriculum may have included aspects cyber warfare, but did contain information operations.

Semesters taught: Although NS410 was offered for 6 years, it was only taught for 3 semesters in each Spring during 2003-2005. Course was recently removed for the 2008-2009 academic year.

Students enrolled: Average enrollment: 5 students.

Infrastructure requirements: Classroom

Audience: NS410 was an elective capstone to the mandatory prerequisite course of NS310 (Strategy and Tactics) now replaced with NS300 (Naval Warfare).

Periodicity issues: NS410 was removed from the course catalog due to low student interest for multiple years. Low accession is presumed to be based off of NS410 being an elective course with a 300 level pre-req. This course also stemmed from a USNA strategic initiative to construct a Netcentric Operational Center and Warfighting Lab in 2003.

Course Number/Title: N/A

The Stockdale Center for Ethical Leadership is discussing moral issues with technology in their Fellows Seminar this year. Cyber warfare may be an interesting ethical leadership discussion.

Appendix B

Questions asked of the sister service academies and cohort civilian undergraduate institutions

- Please describe your “center.” What are the primary goals of your center (student/faculty research, information focal-point, faculty expertise, cyber-funding, organization of guest speakers/lecturers, student extra curricular activities)? Under what organization is your center run (CS-Department, Dean, Provost)? How many faculty are assigned or associated with the “center”? Which of these have a primary duties associated with the "center"? How many labs and/or classrooms are specifically dedicated or associated with the “center”?

- What courses does your “center” provide that currently provide that support or relate to “cyber-warfare”?

  Course number and title
  Department responsible
  Intended audience
  Brief description
  Typical enrollment size
  Lab requirements

- What courses does your institution provide that currently provide that support or relate to “cyber-warfare”?

  Course number and title
  Department responsible
  Intended audience
  Brief description
  Typical enrollment size
  Lab requirements

- For schools with a core course (one required of all or multiple majors): How does the “Center” feed material into these core courses?

- Besides offered courses, are there any other means through which students interact with the “center”?

- How do faculty interact with the "center" (research, funding)?

- What total infrastructure is needed to support all “cyber-warfare”-related course offerings?

  How many classrooms?
  How many labs?

- Please specify which resources, if they did not exist, would prevent the center from accomplishing its goals.
- What resources they would you like to have in order to do more?

- Are there any current issues with respect to facilities?

- What other institutions does the “center” collaborate with?
  civilian institutions
  other cyber institutions
  intelligence communities

- What regular (monthly, annual, semester) events does your "center" facilitate (e.g. Seminars, Conferences, Guest Lectures)?

- Do you have any adjunct or visiting faculty from the intelligence community or an outside organization? If yes, what role do they play?

- What role does your IT Support organization play in meeting the requirements for cyber activities and the "center"? Who acquires/maintains equipment?

- How do you communicate the need for cyber warfare capable graduates (student outcomes, learning objectives)?

- Did you have any issues that you had to overcome in applying for / being accepted as an NSA/DHS Center of Academic Excellence?

Appendix C: USAFA and USMA Cyber Warfare learning objectives

USAFA: Specific learning objectives for the core required USAFA freshman year computer science course include:

- Define information security
- Define risk to information in terms of threats and vulnerabilities
- Define threat and vulnerability
- Describe the three guiding principles of information and the fourth derived principle: confidentiality, integrity, and availability; authentication
- Describe the types of threats to the principles of information security
  - Interruption attacks on Availability
  - Interception attacks on Confidentiality
  - Modification attacks on Data Integrity
  - Fabrication attacks on Authentication
- Describe how the information security principles are implemented to address these threats
  - Availability - redundancy, backups, physical security
  - Confidentiality - encryption, secure channels, steganography
  - Integrity - hash functions, checksums, error-correcting code
  - Authentication - digital signatures, PINs, passwords, biometrics
- Understand how the Navy approaches computer security and appreciate the need for these policies and procedures
- Describe transposition and substitution ciphers and give an example of each
- Describe the Caesar cipher and how it is used
- Describe symmetric-key and asymmetric-key encryption and explain how to use each
- Describe digital signatures and how public-key encryption can be used to implement them
- Define physical and digital steganography and give an example of each
- Describe hash functions and checksums and how they are used to ensure information integrity
- Employ RSA public key encryption for providing confidentiality, authentication, or both
- Understand and apply techniques for developing strong passwords
- Comprehend how dictionary and exhaustive attacks are conducted against passwords

- Defend against social engineering attacks on passwords and identity information
- Calculate the effort and time required for various types of password attacks
- Understand and recognize common attacks against personal computing systems
- Describe common security practices which can improve personal cyber security
- Identify current trends in cyber crime and how they relate to personal computer security
- Explore steps which can improve security on personal computers
- Explore cyber security trends by using SQL injection to
    - Recognize the security weaknesses in common on-line database systems
    - Exploit common weaknesses to access and modify information in a simulated SQL database
    - Explore ways to security information in on-line databases

USMA: Specific learning objectives for the core required USMA IT305 course include those listed below (and constitute approximately 50% of the core USMA course). Note that IT305 has a prerequisite IT105 course that addresses foundational computer science topics prior to cadets taking the IT305 course.

Intellectual Property Issues in Cyberspace
Army Sensors
Biometrics
Implications of Changes in IT
Network Principles and Equipment
Network Protocols
Network Services & Wireless Networks
Network Design I
Network Design II and Communications Principles
Army Communications & Networking Systems
Information Processing on the Battlefield
Network Implementation
Information Dominance
Information Assurance
Information Operations - Reconnaissance
Information Operations - Defensive Operations
Information Operations - Attack

Appendix D: Proposed Computer Science Technical Core Course Learning Objectives

Know

- Identify and define the basic hardware elements of a Von Neumann machine.
- Identify and describe common input/output devices
- Identify and define the key measures of processor performance
- Describe the memory hierarchy
- Identify and define the main functions of an operating system
- Describe how application program interfaces are used.
- Understand the basics of computer networks, and networking protocols.
- Describe how information security principles are implemented to address IA goals:
    - Authentication/non-repudiation - digital signatures, passwords, biometrics
    - Availability - redundancy, backups, physical security
    - Confidentiality - encryption, secure channels, steganography
    - Integrity - hash functions, checksums, error-correcting codes
- Compare basic forms of technology-based attacks on the IA goals such as confidentiality - snooping network traffic; integrity - modifying data in transit; authentication - password cracking programs; availability - DOS attacks ...
- Describe symmetric-key and asymmetric-key encryption
- Describe public-key encryption as used to implement digital signatures
- Define physical and digital steganography and give an example of each
- Describe hash functions and checksums and their role in information integrity
- Describe the actions that occur at each level of the Internet protocol stack.

Comprehend

- Understand computer networks, topologies, hubs, switches, routers, IP Addresses and MAC Addresses (LAN).
- Comprehend binary numbers, binary encoding of text, images
- Comprehend what security is offered by techniques such as 128-bit encryption.
- Comprehend how passwords can be broken by dictionary/exhaustive attacks.
- Comprehend web transaction security as related to http(s), cookies, etc.
- Describe the warning signs of a computer system compromise.
- Analyze Information Assurance mechanisms that aid attainment of IA goals.

Apply

- Employ RSA public key encryption for providing confidentiality, authentication.
- Calculate the effort and time required for various types of password attacks
- Explore cyber security trends impacted by attacks such as SQL injection to
    - Recognize the security weaknesses in common on-line database systems
    - Exploit common weaknesses to access and modify information in a simulated SQL database
    - Explore ways to security information in on-line databases

Demonstrate

- Problem solving and algorithmic thinking as applied to computer programming
- Propose a nominal operational network configuration and associated security protocols that uses appropriate protection mechanisms and employs industry best practices.

References

[1] E. Rosenbach and T. Klajn, “China’s Cyber Warriors,” *The Baltimore Sun*, June 18, 2008, p A11

[2] Editorial, *The Wall Street Journal*, Feb 21, 2009, pg A10

[3] E. Rosenbach and T. Klajn, “China’s Cyber Warriors,” *The Baltimore Sun*, June 18, 2008, p A11

[4] S. Gorman, “New Emphasis on Cyber Security,” *The Wall Street Journal*, Dec 8, 2008, pg A3

[5] A. Cole, “Defense Firms Pursue Cyber-Security Work,” *The Wall Street Journal*, Mar 18, 2009, pg A4

[6] E. Nakashima, “Pentagon Cyber Unit Prompts Questions,” *The Washington Post*, June 13, 2009, p A5

[7] Y.J. Dreazen, “Military Networks Increasingly are Under Attack; US Commander for Cyberspace Says There is China Link,” *The Wall Street Journal*, Mar 12, 2008, pg A7.

[8] CSIS Commission on Cybersecurity for the 44th Presidency, *Securing Cyberspace for the 44th Presidency*, December 2008.

[9] Chairman of the Joint Chiefs of Staff Memorandum of 10 November 2008 titled Definition of Cyberspace Operations

[10] Editorial, *The Wall Street Journal*, Feb 21, 2009, pg A10

[11] E. Rosenbach and T. Klajn, “China’s Cyber Warriors,” *The Baltimore Sun*, June 18, 2008, p A11

[12] OPNAVINST 5239.1C of 20 Aug 09

[13] Chief of Naval Operations Memorandum 5440 Ser N00/100057 of 23 Jul 09.

[14] E. Nakashima, “Pentagon Cyber Unit Prompts Questions,” *The Washington Post*, June 13, 2009, p A5

[15] Memorandum from VADM Dorsett dated June 11, 2009 titled Intelligence/Cyber Update

[16] CJCS Guidance for 2008-2009, available at http://www.jcs.mil/content/files/2009-03/031009163310_CJCS_Guidance_for_2008_2009.pdf

[17] Strategic Initiative Overview based on '*Leaders to Serve the Nation: Our Strategic Plan*', presented at the Naval Academy's Superintendent's Off-site, May 2009.

[18] The Chairman of the Joint Chiefs of Staff, The National Military Strategy for Cyberspace Operations, December 2006. Note that this publication is classified SECRET; the Committee only accessed the UNCLAS portions.

[19] Cooperative Strategy for 21st Century Seapower signed October 2007 signed by CMC, CNO and CCG.

[20] National Defense Strategy signed June 2008 by SECDEF